Saint Louis University Public Law Review

Volume 35
Number 1 *The Thin Blue Line: Policing Post-Ferguson (Volume XXXV, No. 1)*

Article 4

2015

The Fourth Amendment and Bulk Telephone Metadata: An Overview of Recent Case Law

Steven G. Stransky
U.S. Dept of Homeland Security, steven.stransky@hq.dhs.gov

THE FOURTH AMENDMENT AND BULK TELEPHONE METADATA: AN OVERVIEW OF RECENT CASE LAW

STEVEN G. STRANSKY*

I. INTRODUCTION

On June 2, 2015, the President signed into law the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015,[1] which is also known as the "USA FREEDOM Act."[2] The law effectively ended the U.S. government's ability to utilize Section 215 of the USA PATRIOT ACT[3] to collect telephone metadata[4] in bulk from telecommunication service providers for foreign intelligence purposes.[5] On the same day that he signed the USA FREEDOM Act into law, the President issued a statement providing that the law "will strengthen civil liberty safeguards and provide greater public confidence in [the U.S.

* LL.M., National Security Law, Georgetown University Law School; J.D., the University of Akron, C. Blake McDowell Law Center; B.A., The Ohio State University. The author serves as an Attorney-Advisory at the U.S. Department of Homeland Security. The author would like to thank the editors and staff on the Saint Louis University Public Law Review for assisting in the publication of this article. The views and misjudgments contained herein belong entirely to the author.

1. Pub. L. No. 114-23, 129 Stat. 268 (2015). The Bill passed in the House of Representatives by a vote of 388-88 and in the Senate by a vote of 67-32. *See* H.R. 2048, 114th Congress (2015), *available at* www.congress.gov.

2. Judge Mosman described the law's title as "another example of the tail of a catchy nickname wagging the dog of a Rube Goldberg official title." In re Application, Docket No. BR 15-75, at *1, n.1 (FISC Ct. June 29, 2015), redacted opinion *available at* https://www.eff.org/files/2015/07/01/fisa_court_opinion_-_june_29_2015.pdf.

3. P.L. 107-56, 115 Stat. 272 (2001) (codified 50 U.S.C. § 1861).

4. The term "metadata" refers to a set of data or information that describes and gives information about other data, and does not include the content of communications. NAT'L. INFO. SHARING ORG., UNDERSTANDING METADATA 1 (2004), http://www.niso.org/publications/press/UnderstandingMetadata.pdf. (*Understanding Metadata* is a revision and expansion of *Metadata Made Simpler: a guide for libraries* published by NISO Press in 2001.)

5. *See* OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, JOINT STATEMENT BY THE [DEP'T OF JUSTICE] AND THE [OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE] ON THE DECLASSIFICATION OF THE RESUMPTION OF COLLECTION UNDER SECTION 215 OF THE USA PATRIOT ACT (June 30, 2015), http://www.justice.gov/opa/pr/joint–statement–department–justice–and–office–director–national–intelligence–declassificati–0 (noting that "[t]he USA FREEDOM Act of 2015 banned bulk collection under Section 215 of the USA PATRIOT Act . . .").

government's telephone metadata programs,] including by prohibiting bulk collection through the use of Section 215 . . . and by providing the American people with additional transparency measures."[6]

In addition to its distinct statutory amendments limiting the government's ability to collect telephone metadata, the USA FREEDOM ACT will significantly impact on-going litigation concerning the constitutionality of the U.S. government's bulk telephone metadata collection program. Specifically, after certain provisions of the USA FREEDOM ACT go into effect after 180 days of its enactment,[7] the courts will most likely dismiss such litigation on the grounds that that the U.S. government does not have the statutory authority to continue to collect telephone metadata in bulk and the cases will therefore be viewed as moot.[8] According to one commentator, a case pending in the D.C. District Court regarding the government's collection program "will be moot in November when the USA Freedom Act goes into effect."[9] In fact, even prior to the law's passage, "[l]egal scholars" were indicating that "at least three of six major lawsuits against the program likely would be doomed" if the USA FREEDOM Act becomes law, which was troubling to some activists who were relying on these cases to "brand" the government's activities as unconstitutional.[10] According to Professor Douglas Laycock, "[i]t's pretty inconceivable that the Supreme Court would hear one of these cases after a statute makes them moot."[11]

Prior to the USA FREEDOM Act becoming law, however, judges from across the federal judicial system examined whether the U.S. government's collection of bulk telephone metadata was restricted or otherwise impacted by

6. THE WHITE HOUSE, OFFICE OF THE PRESS SECRETARY, *Statement by the President on the* USA FREEDOM Act (June 2, 2015), https://www.whitehouse.gov/the-press-office/2015/06/02/statement-president-usa-freedom-act.

7. *See In re* Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things, No. BR 15-75, at *1 (holding that the USA FREEDOM Act "deliberately carved out a 180-day period following the date of enactment" in which the U.S. government was authorized to continue to use FISA to collect telephone metadata in bulk).

8. *See generally* Steven Nelson, *Freedom Act May Kill Lawsuits That Seek Major Privacy Ruling*, US NEWS & WORLD REP., (May 13, 2015, 5:07 PM), http://www.usnews.com/news/articles/2015/05/13/freedom–act–may–kill–lawsuits–that–seek–major–privacy–ruling.

9. Benjamin Wittes, *Standing Confusion in Obama v. Klayman*, LAWFARE (Aug. 31, 2015, 5:33 PM), https://www.lawfareblog.com/standing–confusion–obama–v–klayman.

10. Nelson, *supra* note 8.

11. Steven Nelson, *Freedom Act's Advance Threatens NSA Court Cases*, US NEWS & WORLD REP. (Nov. 14, 2013, 3:41 PM), http://www.usnews.com/news/articles/2014/11/14/freedom-acts-advance-threatens-nsa-court-cases (quoting Douglas Laycock, Professor, University of Virginia Law School). But see, David Greene, Appeals Court Sends Smith v. Obama NSA Lawsuit Back to the Trial Court, Electronic Frontier Foundation, (Mar. 24, 2016) (noting that certain litigation regarding the U.S. government's metadata collection program may continue to resolve claims for "money damages").

the Fourth Amendment of the U.S. Constitution, and this article consolidates those opinions.[12] In analyzing this constitutional issue, the courts primarily focused on the extent to which the Supreme Court's decision in *Smith v. Maryland*[13] was applicable to the U.S. government's metadata collection efforts and whether the concurring opinions in its more recent decision of *U.S. v. Jones*[14] provided a new framework for analyzing Fourth Amendment matters.[15] However, given the unlikelihood that the courts will continue to accommodate lawsuits regarding the government's (soon to be) obsolete metadata collection program, the case law consolidated herein may provide the only judicial guidance regarding the applicability of the Fourth Amendment and *Smith* and *Jones* with regard to bulk telephone metadata.[16] Thus, to the extent the U.S. government is seeking to establish a new national security program involving the bulk collection of telephone metadata, whether through a separate statutory scheme or through Presidential directive, the cases described *infra* provide the most recent direction and guidance on these Fourth Amendment principles.[17] In other words, although there is a plethora of academic discussions related to the constitutionality of the bulk telephone metadata program, the cases described herein are significant because they represent the only judicial scrutiny on this very narrow topic.[18]

12. *See* United States v. Moalin, No. 10cr4246 JM, slip op., 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013); ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); Smith v. Obama, 24 F.Supp. 3d 1005 (D. Idaho 2014); In re Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13–109, 2013 WL 5741573 (FISA Ct. Aug. 29, 2013). Several courts and commentators have argued that collection of bulk telephone metadata is not authorized by Section 215 of the USA PATRIOT ACT; however, because this article focuses on the judicial decisions regarding the constitutionality of the program, it will only infrequently discuss these statutory arguments.

13. Smith v. Maryland, 442 U.S. 735 (1979).

14. United States v. Jones, 132 S. Ct. 945 (2012).

15. EDWARD C. LIU, ET AL., CONG. RES. SERV., R43459, OVERVIEW OF CONSTITUTIONAL CHALLENGES TO NSA COLLECTION ACTIVITIES 5–6 (2015) (stating that the resolution of this constitutional issue "turns, in large part, on the applicability of the 1979 case *Smith v. Maryland* to the bulk collection program and the persuasiveness of more recent Supreme Court discussions about the effect of new technologies and prolonged government surveillance on the privacy interests of Americans.").

16. *Smith,* 442 U.S. at 735; *Jones*, 132 U.S. at 945. *See also* Part IV infra.

17. *Smith,* 442 U.S. at 735; *Jones*, 132 U.S. at 945.

18. For opposing viewpoints from academia related to the constitutionality of the bulk data collection program, *compare* Randy E. Barnett, Commentary, *The NSA's Surveillance Is Unconstitutional*, THE WALL ST. J. (July 11, 2013, 6:44 PM), http://www.wsj.com/articles/SB100014, *with* Orin S. Kerr, *Metadata, the NSA, and the Fourth Amendment: A Constitutional Analysis of Collecting and Querying Call Records Databases*, THE VOLOKH CONSPIRACY (July 17, 2013, 3:54 AM), http://volokh.com/2013/07/17/metadata-the-nsa-and-the-fourth-amendment-a-constitutional-analysis-of-collecting-and-querying-call-records-databases/.

This article is segregated into five parts. Part II provides a brief overview of the Section 215 bulk telephone metadata collection program. Part III examines the scope of the Fourth Amendment and emphasizes certain judicial precedent and principles that are discussed by the case law described in Part IV; Part III also describes the executive branch's interpretation and application of this Fourth Amendment jurisprudence. Part IV, in turn, discusses the recent case law examining whether the Fourth Amendment applies to the U.S. collection of telephone metadata. As will be described in greater detail below, four separate district courts have ruled directly on this issue and in three of the cases the courts rejected the challenges to the government's collection activities and held that the Supreme Court's precedent in *Smith* supports the conclusion that the U.S. government's collection of telephone metadata in bulk is consistent with the Fourth Amendment.[19] This issue has been discussed (to varying degrees) by two circuit courts, one of which provided, in *dicta*, that the collection of such data raises "serious" constitutional concerns.[20] On the other hand, the Foreign Intelligence Surveillance Court (FISC)[21] has routinely held that this collection activity is consistent with the Fourth Amendment and, in reaching its conclusions, the FISC has addressed the opposing arguments and conclusions reached by the aforementioned district and circuit courts.[22]

II. BACKGROUND: SECTION 215 AND BULK TELEPHONE METADATA

On August 9, 2013, the Obama Administration drafted a "White Paper" that provided, *inter alia*, an overview of its bulk telephone metadata collection program it conducted under Section 215 of the USA PATRIOT ACT.[23]

19. *See* United States v. Moalin, No. 10cr4246 JM, slip op., 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013); *see also* Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013); ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); Smith v. Obama, 24 F. Supp. 3d 1005 (D. Idaho 2014); In re Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13–109, 2013 WL 5741573 (FISA Ct. Aug. 29, 2013).

20. *See* ACLU v. Clapper, 785 F.3d 787 (2d. Cir. 2015); Obama v. Klayman, No. 14-5004 (D.C. Cir. 2015).

21. *See* The Foreign Intelligence Surveillance Act of 1978, as amended (FISA), Pub. 95–511, 92 Stat. 1783 (codified at 50 U.S.C. § 1801–1885c). The FISC is an eleven-judge court that may approve requests from the Attorney General for warrants to authorize the U.S. government to undertake certain surveillance for foreign intelligence purposes. *Id.*

22. *See Moalin*, No. 10cr4246 JM, slip op., 2013 WL 6079518; *see also Klayman*, 957 F. Supp. 2d; *Clapper*, 959 F. Supp. 2d; *Smith*, 24 F. Supp. 3d; *In re Application*, No. BR 13–109, 2013 WL 5741573; *Clapper*, 785 F.3d; *Klayman*, No. 14-5004.

23. ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT (Aug. 9, 2013) [hereinafter, "White Paper"], https://www.eff.org/document/administration–white–paper–section–215–patriot–act. *See generally* Ellen Nakashima & Robert Barnes, *Obama Administration Asserts Broad Surveillance Powers*, WASH. POST, Aug. 10, 2013, *available at* https://www.washingtonpost.com/politics/oba

Therein, the Administration states that "[d]etecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools" in the U.S. government's efforts to combat terrorism, and "[i]t is imperative that [the U.S. government] have the capability to rapidly identify any terrorist threat inside the United States."[24] "One important method that the Government has developed to accomplish this task," according to the White Paper, "is analysis of metadata associated with telephone calls within, to, or from the United States."[25] Not surprisingly, the Director of National Intelligence provided similar comments during congressional testimony as he noted that Section 215 provides an "important tool" in detecting and preventing terrorist attacks.[26]

Section 215 of the USA PATRIOT ACT authorizes the FISC to issue a court order for the "production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism," so long as the investigation of a United States person is not "conducted solely on the basis of activities protected by the first amendment to the Constitution."[27] The White Paper states that pursuant to Section 215, the Federal Bureau of Investigation (FBI) would obtain FISC orders directing telecommunication service providers to give the National Security Agency (NSA) their business records that contain certain telecommunications metadata, such as telephone numbers dialed and the date, time, and duration of a call.[28] The court orders generated by the FISC do not authorize the NSA to "listen to" or "record" any telephone calls as part of this program.[29] Because the telecommunication entities "are directed to supply virtually all of their calling records to the NSA, the [FISC's] orders result in

ma–administration–asserts–broad–surveillance–powers/2013/08/09/ff429504–0134–11e3–96a8–d3b921c0924a_story.html.

24. White Paper, *supra* note 23, at 2.

25. White Paper, *supra* note 23, at 2.

26. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, U.S. INTELLIGENCE COMMUNITY WORLDWIDE THREAT ASSESSMENT TO THE SENATE SELECT COMMITTEE ON INTELLIGENCE (Jan. 29, 2014) (statement for the record from James R. Clapper, Director of National Intelligence).

27. 50 U.S.C. § 1861(a)(1), (c).

28. White Paper, *supra* note 23, at 3 (noting that FISC production orders "do not allow the Government to collect the *content* of any telephone call, or the names, addresses, or financial information of any party to a call" or "cell phone locational information" (emphasis in original)). *But see* THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 27 (Jan. 23, 2014) ("Some information obtained by the NSA under Section 215 could nevertheless provide a general indication of a caller's geographic location. For instance, the area code and prefix of a landline telephone number can indicate the general area from which a call is sent.").

29. White Paper, *supra* note 23, at 1.

the production of call detail records for a large volume of telephone communications."[30] Approximately every ninety days, the FBI files a new application with the FISC requesting that telecommunication service providers be ordered to continue providing this metadata to the NSA for another ninety days.[31]

The NSA retains and queries this bulk metadata for counterterrorism purposes, which the White Paper described as follows:

> Under the FISC orders authorizing the collection, authorized queries may only begin with an "identifier," such as a telephone number, that is associated with one of the foreign terrorist organizations that was previously identified to and approved by the Court. An identifier used to commence a query of the data is referred to as a "seed." Specifically, under Court-approved rules applicable to the program, there must be a "reasonable, articulable suspicion" that a seed identifier used to query the data for foreign intelligence purposes is associated with a particular foreign terrorist organization . . .
>
> Information responsive to an authorized query could include, among other things, telephone numbers that have been in contact with the terrorist-associated number used to query the data, plus the dates, times, and durations of the calls. Under the FISC's order, the NSA may also obtain information concerning second and third-tier contacts of the identifier (also referred to as "hops"). The first "hop" refers to the set of numbers directly in contact with the seed identifier. The second "hop" refers to the set of numbers found to be in direct contact with the first "hop" numbers, and the third "hop" refers to the set of numbers found to be in direct contact with the second "hop" numbers. Following the trail in this fashion allows focused inquiries on numbers of interest, thus potentially revealing a contact at the second or third "hop" from the seed telephone number that connects to a different terrorist-associated telephone number already known to the analyst. Thus, the order allows the NSA to retrieve information as many as three "hops" from the initial identifier. Even so, under this process, only a tiny fraction of the bulk telephony metadata records stored at NSA are authorized to be seen by an NSA intelligence analyst, and only under carefully controlled circumstances.[32]

30. THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 28, at 22.

31. THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 28, at 27. When the FISC approves an application for an order requesting metadata, it issues a "primary order" outlining the scope of data that each telecommunication entity must provide the NSA and the restrictions on how the government can query and disseminate said data. THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 28, at 23. Separately, the FISC produces a "secondary order" addressed to the telecommunication entity directing it to comply with those terms and conditions. THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 28, at 23.

32. White Paper, *supra* note 23, at 3–4. *See also* Exec. Order No. 12333, 40 Fed. Reg. 59,941, 59,949 (Dec. 4, 1981) (describing the limitations on the ability for Intelligence

In addition to how the NSA queries this metadata, the White Paper discusses how this data was retained and disseminated.[33] Specifically, it provides that the "[r]esults of authorized queries are stored and are available only to those analysts trained in the restrictions on the handling and dissemination of the metadata" and "[q]uery results" are further analyzed "only for valid foreign intelligence purposes."[34] The NSA may "provide leads" to the FBI or other Intelligence Community elements; however, for U.S. persons, the NSA may only provide such leads for counterterrorism investigations.[35] In turn, "[i]f the FBI investigates a telephone number or other identifier tipped to it through this program, [it] must rely on publicly available information, other available intelligence, or other legal processes," such as a court order subpoena, "in order to identify the subscribers of any of the numbers that are retrieved."[36]

The White Paper identifies procedural safeguards related to the retention, querying, and dissemination of this metadata.[37] For example, it provides that "[t]echnical controls preclude NSA analysts from seeing any metadata unless it is the result of a query using an approved identifier," and "when the seed identifier is reasonably believed to be used by a U.S. person, the suspicion of an association with a particular foreign terrorist organization cannot be based solely on activities protected by the First Amendment."[38] In addition, it provides that NSA analysts must "apply the minimization and dissemination requirements and procedures specifically set out in the FISC's orders before query results, in any form, [can be] disseminated outside of the NSA."[39] Unless the metadata is identified thought the aforementioned query process, the NSA

Community elements, such as the NSA, to collect, retain, and disseminate information concerning "U.S. persons," as the term is defined therein).

33. *See* White Paper, *supra* note 23.

34. White Paper, *supra* note 23, at 4.

35. White Paper, *supra* note 23, at 4.

36. White Paper, *supra* note 23, at 4 (noting that if, through further investigation, the FBI "develop[ed] probable cause to believe that a number in the United States was being used by an agent of a foreign terrorist organization," it could then "apply to the FISC for an order . . . to authorize interception of the contents of future communications to and from that telephone number.").

37. *See* White Paper, *supra* note 23.

38. White Paper, *supra* note 23, at 3. According to the White Paper, the "reasonable, articulable suspicion" standard "protects against the indiscriminate querying of the collected data." White Paper, *supra* note 23, at 3. However, "[a]s used in other contexts, [reasonable, articulable suspicion] is a less stringent standard than the "probable cause" standard that is required to be satisfied for criminal search warrants or traditional electronic surveillance under FISA." LIU ET AL., *supra* note 15, at 3.

39. White Paper, *supra* note 23, at 3; *see* 50 U.S.C. § 1801(h) (defining the term "minimization procedures").

must delete the information "no later than five years after the agency receives [it]."[40]

The White Paper notes that "although a large amount of metadata is consolidated and preserved by the Government, the vast majority of that information is never seen by any person" and that "[o]nly information responsive to the limited queries that are authorized for counterterrorism purposes is extracted and reviewed by analysts."[41] This sentiment is echoed by the Congressional Research Service (CRS), which provided the following: "[g]enerally, the telephony metadata program has operated by placing few limits on the government's ability to *collect and retain* large amounts of domestic and international telephone records while imposing more stringent restrictions on the government's capacity to *search or make further use* of the collected metadata."[42] "These restrictions," according to the CRS "are not explicitly required by the statutory text of Section 215," but "[i]nstead . . . are delineated as part of the orders the FISC issues pursuant to Section 215."[43]

III. THE FOURTH AMENDMENT

Recent case law analyzing the government's ability to collect and retain bulk telephone metadata for foreign intelligence purposes has primarily focused on the scope of the Fourth Amendment and the third party doctrine, as enumerated in *Smith*.[44] Accordingly, this section provides background information on the Fourth Amendment's legal framework and how it has been interpreted by the Executive Branch. The Fourth Amendment to the U.S. Constitution provides,

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[45]

The Fourth Amendment's applicability to a particular circumstance depends on whether "the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by

40. THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 28, at 25. *See* also White Paper, *supra* note 23, at 3.

41. White Paper, *supra* note 23, at 4. According to the Administration, "[a]lthough the number of unique identifiers has varied substantially over the years, in 2012, fewer than 300 met the "reasonable, articulable suspicion" standard and were used as seeds to query the data after meeting the standard." White Paper, *supra* note 23, at 4.

42. LIU ET AL., *supra* note 15, at 3 (emphasis in original).

43. LIU ET AL., *supra* note 15, at 3.

44. Smith v. Maryland, 442 U.S. 735 (1979).

45. U.S. CONST. amend. IV.

government action."[46] In other words, the Fourth Amendment protection applies only if (1) a person has an actual (subjective) expectation of privacy in the place searched, and (2) that expectation, viewed objectively, is justified under the circumstances.[47] In determining whether an individual may have a constitutionally protected expectation of privacy, the Supreme Court has routinely relied upon the third party doctrine, which refers to "[t]he principle that one has no reasonable expectation of privacy in information that one has voluntarily disclosed to one or more third parties."[48]

In *Smith v. Maryland*, the Supreme Court analyzed the third party doctrine in the context of metadata disclosed to telephone companies during the course of routine telephone calls, and, as noted above, all the cases discussed *infra* focus on the extent to which *Smith* is applicable in the bulk telephone metadata context.[49] The *Smith* case focused on whether the government could request, without a warrant, that a telephone company install a pen register to record the numbers dialed from the telephone at a criminal suspect's residence and use the information derived therefrom in a criminal prosecution.[50] The Court ruled that the numerical information conveyed to the phone company during a routine telephone call, such as the telephone number dialed, is not protected by the Fourth Amendment because there is no legitimate expectation of privacy in such information.[51] The Supreme Court stated that "[t]elephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[52]

Accordingly, the Court found that telephone subscribers do not "harbor any general expectation that the numbers they dial will remain secret."[53] The Supreme Court held that "even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this

46. *Smith*, 442 U.S. at 740.

47. *Id.* (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

48. BLACK'S LAW DICTIONARY (10th ed. 2014). *See* United States v. Miller, 425 U.S. 435, 443 (1976) (holding that the Fourth Amendment does not prevent "the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed").

49. *See* LIU ET AL., *supra* note 15, at 5–6 .

50. *Smith*, 442 U.S. at 737.

51. *Id.* at 739–46. According to the Court, the "petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.' The installation and use of a pen register, consequently, was not a 'search,' and no warrant was required." *Id.* at 745–46.

52. *Id.* at 743; *see generally* Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561, 577-78 (2009).

53. *Smith*, 442 U.S. at 743.

expectation is not 'one that society is prepared to recognize as 'reasonable.'"[54] The Court reiterated that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[55]

The Supreme Court's decision in *United States v. Jones* needs to be discussed herein because of the manner in which it has been incorporated or rejected by the court decisions described *infra*.[56] In *Jones*, law enforcement officers attached, without a warrant, a Global Positioning System (GPS) device to the defendant's vehicle and tracked his location for twenty-eight days.[57] The defendant filed a motion to suppress the evidence derived from this surveillance on the grounds that the government's actions violated protections afforded to him under the Fourth Amendment.[58] The Supreme Court granted *certiorari* to address this issue and Justice Scalia, writing on behalf of the majority, concluded that the law enforcement officers' conduct constituted a search under the Fourth Amendment because the information at issue was obtained by means of a physical intrusion on the defendant's vehicle, which is a constitutionally-protected area.[59]

Two concurring opinions in *Jones*, however, raised concerns with relying upon precedent for analyzing reasonable expectations of privacy in the context of the government's ability to collect information on a person through the use of advanced technological systems.[60] Specifically, in her concurring opinion, Justice Sotomayor questioned the relevancy of *Smith* in analyzing the constitutionality of bulk data collections, and provided the following passage, which garnered special attention in the cases described below:

> "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which

54. *Id.* (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

55. *Id.* at 743–44; *see also* United States v. Reed, 575 F.3d 900, 914 (9th Cir. 2009) (holding "data about [a telephone] 'call origination, length, and time of call' . . . is nothing more than pen register and trap and trace data, [in which] there is no Fourth Amendment 'expectation of privacy'") (quoting *Smith*, 442 U.S. at 743–44); *see also* Gilday v. Dubois, 124 F.3d 277, 296 n.27 (1st Cir. 1997) (quoting *Smith*, 442 U.S. at 743–44).

56. *See* LIU ET AL., *supra* note 15, at 5–6.

57. United States v. Jones, 132 S. Ct. 945, 948; *see generally* Robert Barnes, *Supreme Court Limits Police Use of GPS Tracking*, WASH. POST (Jan. 23, 2012), https://www.washingtonpost.com/politics/supreme-court-warrants-needed-in-gps-tracking/2012/01/23/gIQAx7qGLQ_story.html.

58. *Jones*, 132 S. Ct. at 948.

59. *Id.* at 949, 953. According to Justice Scalia, "[i]t is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted." *Id.* at 949.

60. *Id.* at 955.

> people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[61]

According to Professor Miriam Baer, "in fewer than ten paragraphs, Justice Sotomayor questions and reframes two of the oldest and most criticized doctrines in modern Fourth Amendment jurisprudence," but "[c]ommendably, Justice Sotomayor's opinion stops short of creating the drastic change in Fourth Amendment jurisprudence."[62]

In his concurring opinion, Justice Alito, provided the following guidance with regard to the novel issues associated with using modern, non-intrusive surveillance techniques: "the best that [the Court] can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated."[63] "Under this approach," according to Justice Alito, "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable."[64] However, Justice Alito concluded by noting that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy" and that "[f]or such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[65] It is important to note that in contrast to Justice Sotomayor's concurrence, Justice Alito's concurring opinion does not reference the third party doctrine, the *Smith* case, or government efforts related to the collection or retention of bulk telephone metadata.[66]

A. Executive Branch Interpretation and Application

Since the Judiciary Act of 1789, the primary responsibility of the Attorney General "has been to advise the President and the heads of the executive

61. *Id.* at 955–57 (Sotomayor, J., concurring) (internal citations omitted).

62. Miriam H. Baer, *Secrecy, Intimacy, and Workable Rules: Justice Sotomayor Stakes Out the Middle Ground in United States v. Jones*, 123 YALE L.J. F. 393 (2014).

63. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

64. *Id.*

65. *Id.*

66. *Id.* at 957.

departments on legal matters,"[67] and the Office of Legal Counsel ("OLC") has been "delegated virtually all of the Attorney General's contemporary opinion writing."[68] The OLC itself has stated that it is responsible for providing "authoritative legal advice to the President and all the Executive Branch agencies,"[69] and the courts have recognized that OLC-issued opinions are, except under certain circumstances, "binding as a matter of law" on the Executive Branch.[70] The OLC has previously put forth formal guidance regarding how the Fourth Amendment impacts (1) the government's collection of telephone metadata and (2) intelligence community collection activities, in general.[71] In order to better understand the government's position in the judicial case described *infra*, these two issues will be described here.

First, regarding the collection of telephone metadata, the OLC has consistently held that, in accordance with *Smith*, an individual does not possess a constitutionally protected reasonable expectation of privacy in information provided to telephone companies during the course of routine telephone calls.[72] The OLC relied on this precedent and legal reasoning when interpreting whether an individual has a constitutionally protected reasonable expectation in bulk metadata provided to third parties.[73] Specifically, the OLC has stated,

67. Douglas W. Kmiec, *OLC's Opinion Writing Function: The Legal Adhesive for a Unitary Executive*, 15 CARDOZO L. REV. 337, 337 (1993); *see* 28 U.S.C § 511 ("The Attorney General shall give his advice and opinion on questions of law when required by the President."); *id.* §511 ("The head of an executive department may require the opinion of the Attorney General on questions of law arising in the administration of his department.").

68. Kmiec, *supra* note 67, at 337; *see also* 28 C.F.R. § 0.25 (enumerating the functions of the OLC).

69. *See* U.S. DEP'T. OF JUSTICE, OFFICE OF LEGAL COUNSEL, *About the Office*, www.justice.gov/olc.

70. *See* Public Citizen v. Burke*,* 655 F. Supp. 318, 321–22 (D.D.C. 1987) (holding that with limited exception, "an Attorney General's opinion is binding as a matter of law on those who request it until withdrawn by the Attorney General or overruled by the courts.").

71. *See e.g.* Memorandum from Steven G. Bradbury, Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion–Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch, 33 Op. O.L.C. 1 (2009).

72. *See e.g. id,* at 6 (providing that, in accordance with Smith, there is "no legitimate expectation of privacy in dialing, routing, addressing, and signaling information transmitted to telephone companies"); Transmission by a Wireless Carrier of Information Regarding Cellular Phone User's Physical Location to Public Safety Organizations*,* 20 Op. O.L.C. 315, 319 n.17 (1996) (noting that the "Supreme Court has repeatedly held that a person has no expectation of privacy in information he voluntarily turns over to third parties," such as in telephone numbers dialed"); Fourth Amendment Implication of Military Use of Forward Looking Infrared Radars Technology for Civilian Law Enforcement, 16 Op. O.L.C. 41, 45 n.17 (1992) (affirming that Smith held "the installation and use of a pen register to record telephone numbers . . . was not a search, although the pen register revealed to police telephone numbers that [the defendant] dialed within the privacy of his own home").

73. *See e.g.* Bradbury*, supra* note 71, at 12.

"[a]s for metadata collection . . . we conclude that under the Supreme Court's decision in [*Smith*], the interception of the routing information for both telephone calls and e-mails does not implicate any Fourth Amendment interests."[74]

These historical OLC memoranda are consistent with the current Administration's interpretation of this issue, which was summarized in the White Paper as follows:

> "Although the telephony metadata obtained through Section 215'[s] [bulk telephone metadata collection program] includes, in addition to the numbers dialed, the length and time of the calls and other similar dialing, routing, addressing, or signaling information, under the reasoning adopted by the Supreme Court in *Smith*, there is no reasonable expectation of privacy in such information, which is routinely collected by telecommunications service providers for billing and fraud detection purposes. Under longstanding Supreme Court precedent, this conclusion holds even if there is an understanding that the third party will treat the information as confidential. Nothing in [*Jones*] changed that understanding of the Fourth Amendment."[75]

The Obama Administration has argued that the "scope" of the U.S. government's telephone metadata collection program "does not alter the conclusion that the collection of telephony metadata under a Section 215 court order is consistent with the Fourth Amendment."[76] "Collection of telephony metadata in bulk from telecommunications service providers under the program," according to the Administration, "does not involve searching the property of persons making telephone calls. And the volume of records does not convert that activity into a search."[77]

Second, the OLC has repeatedly held that even if U.S. intelligence community activities impact an individual's constitutionally protected right to privacy, the Fourth Amendment does not always require the government to obtain a warrant in order to effectuate these efforts.[78] For instance, in 2006, the

74. Memorandum from Jack L. Goldsmith, OFFICE OF THE ASSISTANT ATT'Y GEN., REVIEW OF THE LEGALITY OF THE STELLAR WIND PROGRAM 101 (May 6, 2004) [hereinafter, "STELLAR WIND"], redacted memorandum www.justice.gov/sites/default/files/pages/attachments/2014/09/19/may_6_2004_goldsmith_opinion.pdf.

75. White Paper, *supra* note 23, at 20.

76. White Paper, *supra* note 23, at 20.

77. White Paper, *supra* note 23, at 20.

78. *See* Memorandum from Alberto R. Gonzales, Attorney General, U.S. Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President, 30 Op. Att'y Gen. 1, 8 (2006) [hereinafter Legal Authorities] ("[T]he President has inherent constitutional authority to conduct warrantless searches and surveillance within the United States for foreign intelligence purposes."); *see also* STELLAR WIND, *supra* note 74, at 37–43 (arguing that even in peacetime, absent congressional action, the President has inherent constitutional authority, consistent with the Fourth Amendment, to order warrantless foreign intelligence surveillance).

OLC provided the following assessment related to the Fourth Amendment and U.S. intelligence community activities:

> "The touchstone for review of government action under the Fourth Amendment is whether the search is "reasonable" . . . [A]ll of the federal courts of appeals to have addressed the issue have affirmed the President's inherent constitutional authority to collect foreign intelligence without a warrant . . . . Properly understood, foreign intelligence collection in general . . . fit[s] within the "special needs" exception to the warrant requirement of the Fourth Amendment. Accordingly, the mere fact that no warrant is secured prior to the surveillance at issue in the NSA activities does not suffice to render the activities unreasonable."[79]

The OLC has stated that in determining whether a government activity is reasonable within the context of a Fourth Amendment analysis, one must undertake a "general balancing approach, 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'"[80] This OLC interpretation has been reinforced by the current Administration.[81]

IV. THE FOURTH AMENDMENT AND TELEPHONE METADATA: RECENT CASE LAW

In recent years, four district courts, one circuit court, and several FISCs have addressed – to varying degrees – whether the U.S. government's collection and retention of bulk telephone metadata for foreign intelligence purposes is consistent with the Fourth Amendment.[82] This portion of the memorandum describes the legal analysis, reasoning, and conclusions reached by these separate courts on this discrete issue.

79. Legal Authorities, *supra* note 78, at 33; *see also* STELLAR WIND, *supra* note 74, at 37–43 (providing a substantially similar legal analysis).

80. Legal Authorities, *supra* note 78, at 33.

81. *See* White Paper, *supra* note 23, at 21.

82. *See generally* United States v. Moalin, No. 10cr4246 JM, slip op., 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013); *see also* Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013); *see also* ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); *see also* Smith v. Obama, 24 F.Supp. 3d 1005 (D. Idaho 2014); *see also* In re Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13–109, 2013 WL 5741573 (FISA Ct. Aug. 29, 2013); *see also* In re Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-158 (FISA Ct. October 11, 2013), www.aclu.org/files/assets/2013.10.11_fisa_court_memorandum.pdf; *see also* In re Application of F.B.I. for an Order Requiring the Production of Tangible Things, No. BR 14-01 (FISA Ct. March 20, 2014), https://assets.documentcloud.org/documents/1148929/opinion-and-order-in-case.pdf; *see also* In re Application of the F.B.I. for an Order Requiring the Production of Tangible Things, No. BR 15-75 (FISC Ct. June 29, 2015).

A. District Court Decisions

As noted, four separate district courts have ruled directly on the aforementioned issue related to the bulk collection of telephone metadata and in three of the cases the courts have indicated that the third party doctrine, as interpreted by the Supreme Court in *Smith*, is applicable to the U.S. government's collection activities therein.[83] In contrast, only one district court opinion distinguished bulk collection of telephone metadata from the Court's decision in *Smith*, and indicated that such information most likely is protected by the Fourth Amendment.[84]

1. *United States v. Moalin*

In *U.S. v. Moalin*,[85] the U.S. government alleged that the defendants conspired to and provided certain types of material support to terrorists and terrorist organizations in violation of law.[86] Prior to trial, the defendants sought to suppress wiretap evidence obtained pursuant to a FISC warrant on the grounds that the collection of such information violated, *inter alia*, the Fourth Amendment.[87] The court denied the defendants' request to suppress such evidence, and, after seventeen days of trial and deliberations, the jury found the defendants guilty on all counts alleged in the U.S. government's indictment.[88] After the trial, the news media reported on the existence of several classified surveillance programs conducted by the U.S. government, which included the Section 215 program and other programs used to gather information on the defendants.[89] Consequently, the defendants filed a motion for a new trial on the basis that the Fourth Amendment protects the telephone metadata provided to their telecommunication providers, and the U.S. government's collection of such information in bulk violated their constitutional rights.[90] Thus, in reviewing this motion, the court addressed whether the defendants had any reasonable expectation of privacy in certain telephone metadata.[91] At the time the motion for a new trial was filed with the court, one commentator opined,

83. *See* Smith v. Maryland, 442 U.S. 735 (1979).

84. *See Moalin*, 2013 WL 6079518.

85. *Id.*

86. *Id.* at *1.

87. *Id.* at *1, *5.

88. *Id.* at 2–3; *see also* Press Release, FEDERAL BUREAU OF INVESTIGATION, *Three Somali Immigrants Sentenced for Providing Support to Foreign Terrorists* (Nov. 18, 2013).

89. *Moalin*, 2013 WL 6079518 at *3.

90. *Id.* at *5.

91. *Id.*

"if it proves successful, . . . [it will] break the NSA's dragnet phone surveillance program."[92]

Judge Miller, writing the opinion of the district court, began his Fourth Amendment analysis by reiterating the Supreme Court's holding in *Smith* that "someone who uses a telephone has 'voluntarily conveyed numerical information to the telephone company and exposed that information to its equipment in the ordinary course of business,' and therefore has 'assumed the risk that the company would reveal to police the numbers he dialed.'"[93] The Judge then noted that the defendants were requesting the court to ignore precedent, including the *Smith* decision, and to "blaze a new path and adopt the approach to the concept of privacy set forth by Justice Sotomayor in her concurrence in [*Jones*]."[94]

Judge Miller provided, "Justice Sotomayor stated that the recent rise of the digital era of cell phones, internet, and email communications may ultimately require a reevaluation of 'expectation of privacy in information voluntarily disclosed to third parties.'"[95] The "defendants extrapolate from this *dicta*," according to Judge Miller, "that the court should recognize that defendant Moalin had a reasonable expectation of privacy cognizable under the Fourth Amendment that the Government would not collect either individual or aggregated metadata."[96] However, the district court rejected this argument and provided the following:

> "[P]en register-like devices predate the internet era by about 150 years and are not a product of the so-called digital revolution-the basis for the concerns articulated by Justice Sotomayor. Second, and more importantly, the Supreme Court specifically and unequivocally held in *Smith* that retrieval of data from a pen register by the Government without a search warrant is not a search for Fourth Amendment purposes. Because individuals voluntarily convey numerical information to the telephone company to complete a telephone call, one cannot possess a reasonable expectation of privacy in the telephone number dialed (as opposed to the content of the conversation)."[97]

92. Sean Vitka, *The Dragnet's Day in Court*, SLATE (Sept. 30, 2013, 2:25 PM), http://www.slate.com/articles/technology/future_tense/2013/09/basaaly_moalin_s_defense_team_takes_on_ass_nsa_telephone_surveillance.html.

93. *Moalin*, 2013 WL 6079518 at *6 (quoting *Smith*, 442 U.S. at 744).

94. *Id*. at *7.

95. *Id.* (quoting United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring)).

96. *Id.*

97. *Id.* (internal citations omitted); *see also* LIU ET AL., *supra* note 15, at 8 (noting that the *Moalin* court rejected the Defendant's motion for a new trial, and in doing so, "observ[ed] that the use of pen registers, which the Supreme Court upheld in *Smith*, have pre-dated the digital revolution by about 150 years, negating the argument that the *Jones* concurrences' discussion of new technologies compelled a different result").

Judge Miller stated that "when defendant Moalin used his telephone to communicate with third parties, whether in Somalia or the United States, he had no legitimate expectation of privacy in the telephone numbers dialed.[98] The calls were routed through the communications company and its switching equipment in the ordinary course of business."[99] According to the Judge Miller, "[w]hile defendant Moalin may have had some degree of a subjective expectation of privacy, that expectation is not 'one that society is prepared to recognize as reasonable.'"[100] Judge Miller concluded his opinion by referencing similar holdings promulgated by the FISC,[101] which will be discussed in more detail *infra*.

2. *Klayman v. Obama*

In *Klayman v. Obama*,[102] subscribers to certain telecommunications and Internet services brought actions against the U.S. government and private service providers alleging, *inter alia,* that the government's bulk collection of telephone metadata violated the Fourth Amendment.[103] The subscribers moved for a preliminary injunction to prevent the U.S. government from continuing to engage in the bulk collection and querying of telephone record metadata, and to require the government to destroy any such metadata in its possession.[104] In analyzing whether to grant the preliminary injunction, the district court undertook a legal analysis wherein it considered, *inter alia*, whether the plaintiffs have a substantial likelihood of success on the merits, including (germane to the issue herein) whether they are likely to succeed on their Fourth Amendment claim.[105]

Ultimately, based on the following rational, the district court found that *Smith* was not binding precedent in the context of the *Klayman* case and that "bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy."[106] First, Judge Leon, writing on behalf of district court, distinguished the type of bulk data collection undertaken by the government in its case from the facts in *Smith* on the basis that the records used by the government in *Smith* were considered "short-term" and "forward-looking" and the government's collection efforts in *Klayman* involved the

98. *Moalin,* 2013 WL 6079518 at *7.

99. *Id.*

100. *Id.* (quoting *Rakas v. Illinois*, 439 U.S. 128, 143–44 n.12, (1978)).

101. *Id.* at *8 ("The FISC has similarly determined that individuals like Defendant Moalin cannot successfully assert a cognizable Fourth Amendment claim to telephony metadata.").

102. Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded to* Obama v. Klayman, No. 14–5004 (D.C. Cir. 2015).

103. *Id.* at 7.

104. *Id.* at 7–8.

105. *Id.* at 25–43.

106. *Id.* at 32.

"creation and maintenance of a historical database containing five years' worth of data."[107] Second, Judge Leon found that the "relationship between the police and the phone company in *Smith* is *nothing* compared to the relationship that has apparently evolved over the last seven years between the Government and telecom companies," which itself raises Fourth Amendment concerns because of the "formalized policy under which the service provider collects information for law enforcement purposes."[108]

Third, Judge Leon referred to the U.S. government's technological capability to store and analyze bulk telephone metadata as "almost-Orwellian" and noted that it is "unlike anything" previously reviewed by the courts.[109] Thereafter, Judge Leon quoted Justice Sotomayor's concurrence in *Jones* and stated that this technology is "'cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously,' thereby 'evad[ing] the ordinary checks that constrain abusive law enforcement practices: limited police . . . resources and community hostility."[110] Finally, Judge Leon focused on the fact that "[c]ell phones have also morphed into multi-purpose devices,"[111] and argued that "*most importantly,* not only is the Government's ability to collect, store, and analyze phone data greater now than it was in 1979, but the nature and quantity of the information contained in people's telephony metadata is much greater, as well."[112] Thereafter, Judge Leon again quoted Justice Sotomayor's concurring opinion in *Jones* and held that "[the] rapid and monumental shift towards a cell phone-centric culture means that the metadata from each person's phone 'reflects a wealth of detail about her familial, political, professional, religious, and sexual associations,'

107. *Id.*

108. *Klayman*, 957 F. Supp. 2d at 32–33 (emphasis in original). Judge Leon stated, "[i]t's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence-gathering operation with the Government." *Id.* at 33; *see also*, Paul Rosenzweig, *The Lynchpin of the Meta-Data Opinion*, LAWFARE (Dec. 16, 2013) ("Judge Leon dismisses Smith v. Maryland (a case that the FISC considered controlling) on the ground that . . . well . . . it's old.").

109. *Klayman*, 957 F. Supp. 2d at 33.

110. *Id.* (quoting United States v. Jones*,* 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring)).

111. *Id.* at 34. *But see* Orin S. Kerr, *Preliminary Thoughts on Judge Leon's Opinion*, VOLOKH CONSPIRACY (Dec. 16, 2013, 6:45 PM) (emphasis in original) http://volokh.com/2013/12/16/preliminary–thoughts–judge–leons–opinion/ (arguing that it does not matter "that today's phones are combined in a single device with *other* functions" because the government's collection program is "not collecting information about the use of those other functions" and "[i]t is only collecting the same information that was collected in Smith v. Maryland: Information about numbers dialed using the device's telephone functionality and when the call was made").

112. *Klayman*, 957 F. Supp. 2d at 33 (emphasis in original).

that could not have been gleaned from a data collection in 1979."[113] "[T]hese trends," according to the Judge, "have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as reasonable."[114] Judge Leon concluded his Fourth Amendment analysis with the following:

> "Plaintiffs have alleged that they engage in conduct that exhibits a subjective expectation of privacy in the bulk, five-year historical record of their telephony metadata, and I have no reason to question the genuineness of those subjective beliefs. The more difficult question, however, is whether their expectation of privacy is one that society is prepared to recognize as objectively reasonable and justifiable . . . [T]he question that I will ultimately have to answer when I reach the merits of this case someday is whether people have a reasonable expectation of privacy that is violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to high-tech querying and analysis without any case-by-case judicial approval. For the many reasons set forth above, it is significantly likely that on that day, I will answer that question in plaintiffs' favor."[115]

According to one commentator, Judge Leon made a "powerful case" for distinguishing the U.S. government's bulk telephone metadata program from its collection activities as issue in *Smith.*[116]

After determining that the U.S. government's collection of telephone metadata in bulk is a "search" within the meaning of the Fourth Amendment, Judge Leon turned next to whether the search was "reasonable."[117] He began his analysis by stating the well-established principle that warrantless searches by the government are *per se* unreasonable in the context of the Fourth Amendment.[118] Judge Leon recognized, but did not endorse, the U.S. government's argument that the "special needs" exception applies to the facts presented, and held that in order to reach a decision on the matter he must "balance" the privacy expectations of the plaintiff against the interests of the U.S. government "to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context."[119]

113. *Id.* at 36 (quoting *Jones* 132 S. Ct. at 955) (Sotomayor, J., concurring); *see generally* Adam Serwer, *How Sotomayor Undermined Obama's NSA*, MSNBC.COM (Dec. 23, 2013, 5:43 PM), http://www.msnbc.com/msnbc/how–sotomayor–undermined–obamas–nsa.

114. *Klayman*, 957 F. Supp. 2d at 36 (emphasis in original).

115. *Id.* at 37.

116. Benjamin Wittes, *Thoughts on Judge Leon's Section 215 Opinion*, LAWFARE (Dec. 17, 2013, 10:30 AM), https://www.lawfareblog.com/thoughts–judge–leons–section–215–opinion.

117. *Klayman,* 957 F. Supp. 2d at 29–31.

118. *Klayman*, 957 F. Supp. 2d at 37–38; *see Chandler v. Miller*, 520 U.S. 305, 313 (1997) ("To be reasonable under the Fourth Amendment, a search ordinarily must be based on individualized suspicion of wrongdoing.").

119. *Klayman*, 957 F. Supp. 2d at 38 (citing Bd. of Educ. v. Earls, 536 U.S. 822, 830–34, (2002)); *see also* Legal Authorities, *supra* note 78, at 33 (discussing the "special needs" exception

Specifically, Judge Leon analyzed (1) the nature of the privacy interest allegedly compromised by the U.S. government's search, (2) the character of the intrusion imposed on the plaintiffs by the government, and (3) the nature and immediacy of the U.S. government's concerns and the efficacy of the government's collection activities in meeting them.[120]

In analyzing the first two criteria, Judge Leon held that because of the reasons described above, the plaintiffs have a "significant expectation of privacy in an aggregated collection of their telephony metadata covering the last five years, and the NSA's Bulk Telephony Metadata Program significantly intrudes on that expectation."[121] In examining the last criteria, Judge Leon stated that "[g]iven the . . . utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics—I have serious doubts about the efficacy of the metadata collection program . . . "[122] Judge Leon concluded by noting that the "plaintiffs have a substantial likelihood of showing that their privacy interests outweigh the Government's interest in collecting and analyzing bulk telephony metadata and therefore the NSA's bulk collection program is indeed an unreasonable search under the Fourth Amendment."[123] According to Professor Orin Kerr, Judge Leon's opinion in *Klayman*, "[g]ives opponents of the NSA program more fuel to add to the fire, but its legal impact is quite limited because the case now just goes to the court of appeals,"[124] which was vacated and remanded by the appellate court primarily because the plaintiffs failed to establish a substantial likelihood of success on the merits on the issue of standing.[125]

to the Fourth Amendment in the context of U.S intelligence community activities); *see also* STELLAR WIND, *supra* note 74, at 33.

120. *Klayman*, 957 F. Supp. 2d at 38.

121. *Id.* at 39.

122. *Id.* at 40–41; *but see* THE WHITE HOUSE, OFFICE OF THE PRESS SECRETARY, *Remarks by President Obama and German Chancellor Merkel in Joint Press Conference* (June 19, 2013, 12:46 p.m.), https://www.whitehouse.gov/the-press-office/2013/06/19/remarks-president-obama-and-german-chancellor-merkel-joint-press-confere (noting that because of the U.S. government's surveillance programs, "at least 50 threats . . . have been averted").

123. *Klayman*, 957 F. Supp. 2d at 41.

124. Ellen Nakashima & Ann E. Marimow, *Judge: NSA's Collecting of Phone Records is Probably Unconstitutional*, Wash. Post (Dec. 16, 2013) (quoting Orin S. Kerr), https://www.washingtonpost.com/national/judge–nsas–collecting–of–phone–records–is–likely–unconstitutional/2013/12/16/6e098eda–6688–11e3–a0b9–249bbb34602c_story.html.

125. Klayman, 800 F. 3d at 561-64.

3. *American Civil Liberties Union v. Clapper*

In *American Civil Liberties Union v. Clapper*,[126] the plaintiffs brought a legal action seeking a declaratory judgment that the NSA's bulk telephony metadata collection program violated, *inter alia*, the Fourth Amendment.[127] The plaintiffs moved for a permanent injunction enjoining the U.S. government from continuing the collection, and, in response, the government moved to dismiss the case.[128]

In analyzing the Fourth Amendment issue, Judge Pauley III, writing on behalf of the district court, reaffirmed the "bedrock holding" articulated in *Smith* that an "individual has no legitimate expectation of privacy in information provided to third parties."[129] Judge Pauley III then continued his opinion to address and then dismiss the plaintiff's argument that protections enumerated within the Fourth Amendment apply to bulk telephone metadata provided to and maintained by telecommunication service providers.[130] According to Judge Pauley III, "the business records created by Verizon are not 'plaintiffs' call records,'" as argued by the Plaintiffs, but are records created and maintained by the telecommunications provider, and "[u]nder the Constitution, that distinction is critical because when a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information."[131] Additionally, "the Government's subsequent querying of the telephony metadata does not implicate the Fourth Amendment—anymore than a law enforcement officer's query of the FBI's fingerprint or DNA databases to identify someone."[132] "The collection of breathtaking amounts of information unprotected by the Fourth Amendment," according to Judge Pauley III, "does not transform that sweep into a Fourth Amendment search."[133]

126. ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) *rev'd on other grounds*; ACLU v. Clapper, 785 F.3d 787 (2d. Cir. 2015) (vacating the district court's rulings on statutory ground, and only briefly discussed the Constitutional issues ruled on by the district court).

127. *Id.* at 730; *see generally* Adam Liptak and Michael S. Schmidt, *Judge Upholds N.S.A.'s Bulk Collection of Data on Calls*, N.Y. TIMES (Dec. 27, 2013), http://www.nytimes.com/2013/12/28/us/nsa–phone–surveillance–is–lawful–federal–judge–rules.html; *see generally* Bob Van Voris, *NSA Call Data Sweep Ruled Legal as Court Conflict Brews*, BLOOMBERG BUSINESS (Dec. 28, 2013, 11:01 PM), http://www.bloomberg.com/news/articles/2013–12–27/nsa–call–data–program–ruled–lawful–by–u–s–judge.

128. *Clapper*, 959 F. Supp. 2d at 730.

129. *Id.* at 749 (citing Smith v. Maryland, 442 U.S. 735 (1979)).

130. *Id.* at 749–52.

131. *Id.* at 751.

132. *Id.*

133. *Id.* at 752; *see also* White Paper, *supra* note 23, at 20 ("Collection of telephony metadata in bulk from telecommunications service providers under the program does not involve searching the property of persons making telephone calls. And the volume of records does not convert that activity into a search.").

In additional, Judge Pauley III critiqued the plaintiff's reliance on Judge Sotomayor's concurrence in *Jones* in formulating their argument:

> The ACLU's reliance on the concurring opinions in *Jones* is misplaced. In *Jones,* the police attached a GPS tracking device to the undercarriage of a vehicle without a warrant and tracked the vehicle's location for the next four weeks. The majority held that a "search" occurred because by placing the GPS device on the vehicle, "[t]he Government physically occupied private property for the purpose of obtaining information . . . [S]uch a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." In two separate concurring opinions, five justices appeared to be grappling with how the Fourth Amendment applies to technological advances.
>
> But the Supreme Court did not overrule *Smith.* And the Supreme Court has instructed lower courts not to predict whether it would overrule a precedent even if its reasoning has been supplanted by later cases . . . Clear precedent applies because *Smith* held that a subscriber has no legitimate expectation of privacy in telephony metadata created by third parties. Inferior courts are bound by that precedent.[134]

Thereafter, Judge Pauley III addressed Judge Leon's opinion in *Klayman*,[135] which, according to the Judge, focused on the "the ubiquity of cellular telephones" and how the relationships between telephone users and telecommunication providers "have evolved since *Smith.*"[136] However, according to Judge Pauley III, this relationship "has not changed and is just as frustrating."[137] Further, the Judge found that it is immaterial to the Fourth Amendment that telephones are more "versatile now than when Smith was decided," because the underlying issue is still focused on the non-communications content aspect of telephone calls.[138] "The fact that there are more calls placed," said Judge Pauley III, "does not undermine the Supreme

134. *Clapper*, 959 F. Supp. 2d at 752 (internal citations omitted); *see* Peter Margulies, *Judge Pauley's Opinion in Clapper: Reset Button for Bulk Collection Debate?* LAWFARE (Dec. 28, 2013, 8:00 AM), https://www.lawfareblog.com/judge–pauleys–opinion–clapper–reset–button–bulk–collection–debate (stating that in Judge Pauley III's view, the warrant requirement, as articulated in *Jones*, for "planting a GPS device" on a car "does not discredit the third-party doctrine" and "*Jones* . . . merely requires a heightened standard for the physical, more comprehensive intrusion connoted by the surveillance in that case, which has none of the elements of consent that drive the third-party doctrine").

135. Liptak & Schmidt, *supra* note 127 (quoting Orin S. Kerr). According to Professor Kerr, the opinions written by Judge Pauley III and Judge Leon are "the exact opposite . . . in every way, substantively and rhetorically." *Id.*

136. *Clapper*, 959 F. Supp. 2d at 752.

137. *Id.*

138. *Id.*

Court's finding that a person has no subjective expectation of privacy in telephony metadata."[139]

Last, Judge Pauley III quoted the *Klayman* decision when concluding his own Fourth Amendment analysis: "[i]mportantly, 'what metadata is has not changed over time,' and '[a]s in *Smith,* the *types* of information at issue in this case are relatively limited: [tele]phone numbers dialed, date, time, and the like."[140] According to Judge Pauley III, "[b]ecause *Smith* controls, the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment."[141] Professor Margulies stated that judge Pauley's opinion "is a welcome corrective to the anti-metadata clamor triggered by Judge Leon's *Klayman* opinion" and it "deflates the overblown arguments made by metadata critics on the program's efficacy, the quality of judicial and congressional oversight, and the continued vitality of the Supreme Court's precedent in *Smith v. Maryland*."[142] However, as will be discussed *infra*, the Second Circuit Court of Appeals overturned this decision, but did so based upon statutory grounds and only addressed the Fourth Amendment issues in *dicta*.[143]

4. *Smith v. Obama*

Similar to the facts discussed in the previous two cases, in *Smith v. Obama*[144] the plaintiff brought an action against the U.S. government wherein she sought a preliminary injunction prohibiting the NSA from collecting her cellular telephone records and call data.[145] Specifically, the plaintiff alleged that the collection activity violated her Fourth Amendment right to be free from unreasonable search and seizure.[146] In response to the plaintiff's motion (and as could be expected), the U.S. government sought to dismiss the case.[147]

Chief Judge Winmill, writing for the district court, analyzed the government's activity within the context of the Fourth Amendment and first reiterated the *Smith* decision and found that the plaintiff "has no expectation of

139. *Id. See also* Kerr, *supra* note 111 (arguing that the change in cell phone use and technology does not alter the underlying conclusions in *Smith*).

140. *Clapper*, 959 F. Supp. 2d at 752 (quoting *Klayman*, 957 F.Supp.2d at 35) (emphasis in original).

141. *Id.*

142. Margulies, *supra* note 134.

143. Smith v. Obama, 24 F.Supp. 3d 1005 (D. Idaho 2014).

144. *Id.*

145. *Id.* at 1006–07.

146. *Id.*

147. *Id. See generally* Orin S. Kerr, *Another Federal Judge Rules on Legality of NSA Surveillance*, WASH. POST (June 3, 2014), https://www.washingtonpost.com/news/volokh–conspiracy/wp/2014/06/03/another–federal–judge–rules–on–legality–of–nsa–surveillance/; Steven Nelson, *Nurse's NSA Lawsuit Gains Firepower*, US NEWS & WORLD REPORT (July 16, 2014), http://www.usnews.com/news/articles/2014/07/16/idaho–nurses–nsa–lawsuit–gains–firepower–from–aclu–eff.

privacy in the telephone numbers that she dials" and "[a] person using the telephone 'voluntarily convey[s] numerical information to the telephone company' and 'assume[s] the risk that the company [will] reveal to police the numbers he dialed.'"[148] Thereafter, Chief Judge Winmill posed a hypothetical question to himself: "the data collected by the NSA reaches into [plaintiff's] personal information [and] the NSA's collection of the time and duration of phone calls is revealing: Would most citizens want to keep private the fact that they called someone at one in the morning and talked for an hour or two?"[149] The Chief Judge went a step further and indicated that the "intrusion" the Supreme Court addressed within *Smith* – law enforcement surveillance of telephone numbers dialed from a criminal suspect for two days – represents a "looming gulf" with the intrusion in the current case,[150] which he described as the U.S. government collecting and storing the telephone metadata of U.S. citizens for five years[151] that results in a "vast trove of data" within the U.S. government's possession.[152] Yet, in response to the concerns he raised, the Chief Judge noted that the Ninth Circuit Court of Appeals has consistently found that telephone and email metadata and other similar information does not receive Fourth Amendment protection[153] and that two other district courts – *Moalin* and *Clapper* – have applied *Smith* to find that the U.S. government's bulk telephone metadata program does not violate the Fourth Amendment.[154]

Next, the Chief Judge addressed Judge Leon's contrary holding in *Klayman*, which he described as a "thoughtful and well-written decision."[155] Chief Judge Winmill provided the following summary of the *Klayman* decision:

> [Judge Leon] distinguished *Smith* by finding that the scope and duration of the NSA's collection is far beyond the individual pen register at issue in *Smith.* Of critical importance to Judge Leon was that *Smith* could never have anticipated the ubiquity of cell-phones and the fact that "people in 2013 have an entirely different relationship with phones than they did thirty-four years ago." As he eloquently observes, "[r]ecords that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and

148. *Smith*, 24 F.Supp. 3d at 1007 (quoting Smith v. Maryland, 442 U.S. 735, 744 (1979)).

149. *Id.* at 1007–08.

150. *Id.* at 1008.

151. *Id.* at 1006–07.

152. *Id.* at 1007.

153. *Id.* at 1008 (citing United States v. Reed*,* 575 F.3d 900, 914 (9th Cir. 2009)); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008); United States v. Golden Valley Elec. Ass'n, 689 F.3d 1108, 1116 (9th Cir. 2012).

154. *Smith,* 24 F. Supp. 3d at 1005; *see generally* Devlin Barrett, *Idaho Judge Asks Supreme Court to End NSA's Phone Surveillance,* WALL ST. J (June 3, 2014, 5:07 PM), http://www.wsj.com/articles/idaho-judge-suggests-supreme-court-end-nsa-phone-surveillance-1401824175.

155. *Smith*, 24 F. Supp. 3d at 1009.

> constantly updating picture of the person's life." Ultimately, he held that the plaintiffs had a likelihood of success on their Fourth Amendment claim, and he enjoined the NSA from collecting their telephone records . . . .[156]

The Chief Judge believes that "Judge Leon's decision should serve as a template for a Supreme Court opinion."[157] Yet, regardless of his admiration for Judge Leon's opinion in *Klayman*, Chief Judge Winmill found that "*Smith* was not overruled, and it continues . . . to bind this Court" and thus "constrains [him] from joining *Klayman.*"[158] Accordingly, the district court granted the defendants' motion to dismiss.[159] Professor Kerr summarized the opinion as follows: "Judge Winmill concludes that the NSA program complies with the Fourth Amendment as a matter of precedent, but . . . expresses the view that the Ninth Circuit and the Supreme Court should change their precedent so as to deem the NSA program unconstitutional."[160]

B. The Circuit Court Decisions

There have been only two circuit courts – the Second Circuit and the District of Columbia Circuit – that have addressed or otherwise discussed whether the U.S. government's collection of bulk telephone metadata for foreign intelligence purposes is consistent with the Fourth Amendment.[161] The Second Circuit's decision primarily focused on statutory matters, but addressed the aforementioned issue in *dicta*.[162] On the other hand, the D.C. Circuit opinion focused on whether the plaintiffs have standing and the thresholds for a preliminary injunction; the D.C. Circuit only mentioned the Fourth Amendment issue in passing.[163] Accordingly, only the Second Circuit opinion will be discussed herein.

1. The Second Circuit: *American Civil Liberties Union v. Clapper*

As noted above, the Second Circuit Court of Appeals discussed the U.S. government's collection of bulk telephone metadata in the context of the Fourth Amendment, [and stated in *dicta*] that the aforementioned government

156. *Id.* (internal citations omitted).

157. *Id.*

158. *Id.* at 1010.

159. *Id.* at 1010.

160. Kerr, *supra* note 147.

161. *See* ACLU v. Clapper, 785 F.3d. 787, 825 (2nd Cir. 2015); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013)561–64 (D.C. Cir. 2013).

162. *See Clapper*, 785 F.3d. at 825.

163. *Klayman*, 800 F.3d at 561–64 ("The preliminary injunction entered by the district court is hereby vacated and the case is remanded for such further proceedings as may be appropriate."). *See generally* Wittes, *supra* note 9 (discussing the *Klayman* ruling on the issue of standing).

activity raises "serious" constitutional concerns.[164] Specifically, on September 2, 2014, the Second Circuit reviewed the appeal from the plaintiffs–appellants wherein they argued that Judge Pauley III, in the decision discussed *supra*, erroneously dismissed their case.[165] At the circuit court, the plaintiffs alleged that the bulk telephone metadata collection program conducted by the U.S. government was not authorized by statute and violated the Fourth Amendment.[166] Judge Lynch, writing on behalf of the Second Circuit, based his decision solely on the former: "[b]ecause we find that the [NSA] program exceeds the scope of what Congress has authorized, we vacate the decision below dismissing the complaint without reaching appellants' constitutional arguments."[167]

However, although Judge Lynch did not use the Fourth Amendment as a basis for his ruling, he did discuss Fourth Amendment concerns at length in *dicta*.[168] Judge Lynch framed the competing constitutional arguments between the parties as follows:

> The government argues, and the district court held, that [the third party] doctrine requires rejection of appellants' claim that the acquisition of telephone metadata (as opposed to the contents of communications) violates the Fourth Amendment, or even implicates its protections at all. Appellants respond that modern technology requires re-visitation of the underpinnings of the third-party records doctrine as applied to telephone metadata.[169]

According to Judge Lynch, this "touches an issue on which the Supreme Court's jurisprudence is in some turmoil."[170] Thereafter, he reiterated the holding in *Smith* related to the third patty doctrine and telephone metadata, but provided the following observation:

> Metadata today, as applied to individual telephone subscribers, particularly with relation to mobile phone services and when collected on an ongoing basis

164. *Clapper*, 785 F.3d at 808; *see generally* Pete Williams, *Federal Appeals Court Says NSA Phone Records Program Illegal*, NBC NEWS (May 7, 2015, 10:08 AM), http://www.cnbc.com/2015/05/07/federal-appeals-court-says-nsa-phone-records-program-illegal-dj.html; Mark Rodgers, *2nd Circuit Finds NSA's Bulk Metadata Program Not Authorized By Patriot Act*, LEXISNEXIS (May 7, 2015, 3:47 PM), http://www.lexisnexis.com/legalnewsroom/technology/b/cyber-risk-privacy/archive/2015/05/07/second-circuit-finds-nsa-s-bulk-metadata-program-not-authorized-by-patriot-act.aspx.

165. *Clapper*, 785 F.3d at 792. *But see* Peter Margulies, *Clapper and the Costs of Overlooking Use Restrictions*, LAWFARE (May 14, 2015, 2:55 PM), https://www.lawfareblog.com/clapper-and-costs-overlooking-use-restrictions (discussing some of the "flaws" in the Second Circuit's decision).

166. *Clapper*, 785 F.3d at 792, 799.

167. *Id.* at 792.

168. *Id*. at 822–25.

169. *Id.* at 822.

170. *Id.* at 821; Rodgers, *supra* note 164 (briefly discussing the constitutional issues raised in the Second Circuit's decision in Clapper).

> with respect to all of an individual's calls (and not merely, as in traditional criminal investigations, for a limited period connected to the investigation of a particular crime), permit something akin to the 24–hour surveillance that worried some of the Court in *Jones.* Moreover, the bulk collection of data as to essentially the entire population of the United States, something inconceivable before the advent of high-speed computers, permits the development of a government database with a potential for invasions of privacy unimaginable in the past. Thus, appellants argue, the program cannot simply be sustained on the reasoning that permits the government to obtain, for a limited period of time as applied to persons suspected of wrongdoing, a simple record of the phone numbers contained in their service providers' billing records.[171]

Judge Lynch concluded his opinion by noting that the court does not need to resolve the "weighty constitutional issues" present in this case, but that "[t]he seriousness of the constitutional concerns" described in the court's opinion "has some bearing on what we hold today, and on the consequences of that holding."[172]

C. Foreign Intelligence Surveillance Court (FISC) Decisions

As noted above, the FISC has routinely addressed the issue of whether bulk metadata collection implicates the Fourth Amendment, although these opinions are not, at least generally speaking, available to the general public.[173] Chief Judge Pauley III noted in his 2013 decision described *infra* that "[f]ifteen different FISC judges have found the metadata collection program lawful a total of thirty-five times since May 2006."[174] Additionally, in ruling upon whether bulk telephone metadata is protected within the scope of the Fourth Amendment, recent FISC decisions have addressed the opposing arguments raised by Judge Leon in *Klayman* and by the Second Circuit in *Clapper*.[175] This portion of the article highlights four of these publicly available FISC decisions, each of which analyzed the Fourth Amendment in the context of the U.S. government's ability to collect bulk telephone metadata.

1. *In re Application* (August 2013 Opinion)

The genesis of *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted]*,[176] can be traced to an application submitted by the FBI on July 18, 2013 to the

171. *Clapper*, 785 F.3d at 824.

172. *Id.*

173. *See* 50 U.S.C. § 1861(c)(1) (2015) (authorizing FISC judges to issue *ex parte* orders approving the release of tangible things).

174. *Clapper*, 959 F. Supp. 2d at 756.

175. In re Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13–109, 2013 WL 5741573, at *9 (FISA Ct. Aug. 29, 2013).

176. *Id.* at *1.

FISC for an order pursuant to 50 U.S.C § 1861, which required the ongoing daily production to the NSA of certain telephone metadata.[177] The FISC "held an extensive hearing to receive testimony and evidence on this matter," which was conducted *ex parte* under security procedures mandated by law;[178] the court approved the application on July 19, 2013.[179] As noted by the Washington Post, the August 2013 opinion "is the first to be released [to the general public] that addresses the constitutionality of the NSA's 'bulk records' collection of phone data," [and was] an attempt by the U.S. government to "address growing criticism about [its] broad surveillance [program] . . . ."[180]

During its review of the government's FISA application, the FISC analyzed whether the Fourth Amendment "imposed any impediment" to the government's proposal to collect bulk telephone metadata.[181] Judge Eagan, writing on behalf of the FISC, noted that the government's collection of telephone service provider metadata is "squarely controlled" by *Smith* and its progeny.[182] According to the FISC Judge, "[t]he Supreme Court in *Smith* recognized that telephone companies maintain call detail records in the normal course of business for a variety of purposes"[183] and "'[t]elephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.'"[184] Thus, "once a person has transmitted this information to a third party (in this case, a telephone company), the person 'has no legitimate expectation of privacy in [the] information,'"[185] and when the

177. *Id.*

178. *Id.*; *see* 50 U.S.C § 1803 (2015) (mandating that FISC proceedings "be maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence"); *see also* Letter from Reggie B. Walton, Presiding Judge, to Patrick J. Leahy, Commissioner, Senate Judiciary Committee (July 29, 2013), http://www.leahy.senate.gov/imo/media/doc/Honorable%20Patrick%20J%20Leahy.pdf (describing some of the security measures implemented by the FISC).

179. *In re Application*, WL 5741573 at *1.

180. Ellen Nakashima, *FISA Court Releases Opinion Upholding NSA Phone Program*, WASH. POST (Sept. 17, 2013), https://www.washingtonpost.com/world/national-security/fisa-court-releases-opinion-upholding-nsa-phone-program/2013/09/17/66660718-1fd3-11e3-b7d1-7153ad47b549_story.html.

181. *In re Application*, WL 5741573 at *1.

182. *Id*. at *2; *see generally* Benjamin Wittes & Jane Chong, *Congress Has No Clothes: A Quick and Dirty Summary of the New FISC Opinion*, LAWFARE (Sept. 17, 2013, 9:03 PM), https://www.lawfareblog.com/congress-has-no-clothes-quick-and-dirty-summary-new-fisc-opinion (noting that Judge Eagan put forth a "strong" legal opinion).

183. *In re Application*, WL 5741573 at *2 (citing Smith v. Maryland, 442 U.S. 735, 742 (1979)).

184. *Id.* (quoting *Smith*, 442 U.S. at 743).

185. *Id.* (quoting *Smith*, 442 U.S. at 743).

government obtains this telephone metadata from the telephone company, it is not conducting a "search," within the meaning of the Fourth Amendment.[186]

Judge Eagan considered the factual distinctions between *Smith* and more recent requests by the U.S. government to collect telephone metadata in bulk.[187] She recognized that *Smith* focused on the government's ability to obtain "the telephone company's metadata of one person suspected of a crime" and the current case focused on the government's request for the "daily production of certain telephony metadata in bulk belonging to companies without specifying the particular number of an individual."[188] Judge Eagan cited a similar (but redacted) legal analysis that the FISC had previously undertaken, and noted that "the application of the Fourth Amendment depends on the government's intruding into some individual's reasonable expectation of privacy [and] Fourth Amendment rights are personal and individual."[189] Thus, "[s]o long as no individual has a reasonable expectation of privacy in meta data, the large number of persons whose communications will be subjected to the . . . surveillance is irrelevant to the issue of whether a Fourth Amendment search or seizure will occur."[190]

Judge Eagan reinforced her legal analysis by stating, "where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*."[191] In other words, "Judge Eagan concludes that if metadata does not implicate an individual's Fourth Amendment privacy interest in his telephony metadata, neither does the bulk collection of metadata about numerous persons."[192]

In concluding her opinion, Judge Eagan stated that because the U.S. government's application only concerns the production of telephony metadata that was collected and retained by a telecommunications provider – and not the contents of communications – the *Smith* decision "compels the conclusion that there is no Fourth Amendment impediment to the collection."[193] According to the Judge, "this Court finds that the volume of records being acquired does not

186. *Id.* (citing *Smith*, 442 U.S. at 746); *see generally* Orin S. Kerr, *My (Mostly Critical) Thoughts on the August 2013 FISC Opinion on Section 215*, VOLOKH CONSPIRACY (Sept. 17, 2013, 7:39 PM), http://volokh.com/2013/09/17/thoughts-august-2013-fisc-opinion-section-215/ (briefly noting support for Judge Eagan's Fourth Amendment analysis).

187. *In re Application*, WL 5741573 at *2–3.

188. *Id.* at *2.

189. *Id.*

190. *Id. See also* White Paper, *supra* note 23, at 20 (addressing whether the volume of records impacts the Fourth Amendment analysis regarding bulk telephone metadata).

191. *In re Application*, WL 5741573 at *2.

192. Wittes & Chong, *supra* note 182.

193. *In re Application*, WL 5741573 at *3.

alter this conclusion" and "there is no legal basis for this Court to find otherwise."[194]

2. *In re Application* (October 2013 Opinion)

On October 11, 2013, Judge McLaughlin of the FISC granted the FBI's application to renew the order discussed in the aforementioned August 2014 FISC ruling.[195] She issued a memorandum that both adopted Judge Eagan's conclusions regarding the Fourth Amendment and provided additional reasoning that supported her argument that the production of bulk telephone metadata does not implicate the Fourth Amendment.[196] Judge McLaughlin began her Fourth Amendment analysis by noting that she "agrees with Judge Eagan that, under [*Smith*], the production of call detail records in this matter does not constitute a search under the Fourth Amendment."[197] Judge McLaughlin found that the Supreme Court "stressed" in *Smith* that the U.S. government's use of a pen register to record the numbers dialed from the defendant's home telephone did not constitute a "search" within the meaning of the Fourth Amendment because "the information acquired did not include the contents of any communication and that the information was acquired by the government from the telephone company, to which the defendant had voluntarily disclosed it for the purpose of completing his calls."[198]

According to the New York Times, "Judge Eagan's opinion," discussed *infra* "has been criticized, in part, because she made no mention of a landmark privacy case decided by the Supreme Court in 2012,"[199] and, in contrast Judge McLaughlin specifically addressed the *Jones* decision and found that it "does not point to a different result here."[200] More specifically, Judge McLaughlin reiterated the holding in *Jones* and stated the majority opinion of the Court "declined to decide whether use of the GPS device, without the physical intrusion, impinged upon a reasonable expectation of privacy."[201] Judge McLaughlin stated that although "[f]ive Justices in *Jones* signed or joined concurring opinions suggesting that the precise, pervasive monitoring by the government of a person's location could trigger Fourth Amendment protection

194. *Id.*

195. In re Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-158, at *1–2 (FISA Ct. October 11, 2013), *available at* www.aclu.org/files/assets/2013.10.11_fisa_court_memorandum.pdf. *See generally* Charlie Savage, *N.S.A. Plan to Log Calls Is Renewed by Court*, N.Y. TIMES (Oct. 18, 2013), http://www.nytimes.com/2013/10/19/us/nsa-plan-to-log-calls-is-renewed-by-court.html.

196. *In re Application*, No. BR 13-158, at *4–5.

197. *Id*. at *4.

198. *Id.*

199. Savage, *supra* note 195.

200. *In re Application*, No. BR 13-158, at *4.

201. *Id.*

even without any physical intrusion[,]" the issue presented for her review (i.e., the collection of bulk telephone metadata) does not involve such monitoring, and, "[l]ike *Smith*, this case concerns the acquisition of non-content metadata other than location information."[202]

She also addressed Judge Sotomayor's concurring opinion in *Jones*, which provided that "it 'may be necessary' for the Supreme Court to 'reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties,' which [the Associate Supreme Court Justice] described as 'ill suited to the digital age.'"[203] Judge McLaughlin emphasized in her FISC opinion, however, that the *Jones* case did not actually re-examine the relevancy of the third party doctrine,[204] and that "*Smith* remains controlling with respect to the acquisition by the government from service providers of non-content telephony metadata."[205]

3. *In re Application* (March 2014 Opinion)

On January 3, 2014, the FISC issued an order requiring telecommunication entities to produce to the NSA, in bulk and on an ongoing basis, certain metadata within their possession.[206] On January 22, 2014, a recipient of the production order filed a petition with the FISC requesting the court "to vacate, modify, or reaffirm" said order in light of the conclusions reached by Judge Leon in *Klayman*.[207] According to one commentator, "[t]he petition was the first time a telephone company had directly challenged an order to hand over phone records in bulk."[208] In response, the U.S. government filed a reply brief to the FISC that noted that the FISC, in issuing its original production order, did in fact consider *Klayman*, as well as the FISC's holdings in its August

202. *Id.* at *5. *See also* Allison Grande, *FISA Judge Renews NSA Spying, Citing Congress' Support*, LAW360 (Oct. 21, 2013, 4:33 PM) (noting that Judge McLaughlin "rejected the argument" that the NSA's telephone metadata collection program "violates the Fourth Amendment, finding that the production of metadata on domestic phone calls does not constitute a 'search' because it does not include the contents of conversations and the data is collected directly from a telephone company to which consumers voluntarily disclose their information").

203. *In re Application*, No. BR 13-158, at *5 (quoting United States v. Jones, 132 S. Ct., 945, 957 (2012) (Sotomayor, J., concurring)).

204. *Id*. ("The Supreme Court may some day revisit the third-party disclosure principle in the context of twenty-first century communications technology, but that day has not arrived.").

205. *Id*. at *5–6.

206. In re Application of F.B.I. for an Order Requiring the Production of Tangible Things, No. BR 14-01, *1 (FISA Ct. March 20, 2014), https://assets.documentcloud.org/documents/1148929/opinion-and-order-in-case.pdf.

207. *Id.* at *1–2. In accordance with FISA, the recipient of a FISC production order is permitted to "challenge the legality of that order" with the FISC. *Id.* at *1 (citing 50 U.S.C. § 1861(f)(2)(A)(i) (2015); FISC Rule 33(a) (2010)).

208. Julian Hattem, *Phone Company Fought NSA — and Lost*, THE HILL (April 25, 2014, 6:19 PM), http://thehill.com/policy/technology/204438-phone-company-challenged-nsa-program-lost.

2013 and October 2013 decisions, respectively.[209] Judge Collyer, writing on behalf of the FISC, affirmed the production order and noted that it "remains in full force and effect until it expires by its own terms on March 28, 2014,"[210] and discussed at length whether the Fourth Amendment impacts the U.S. government's ability to collect telephone metadata in bulk.[211] Judge Collyer's legal analysis can be separated into three sections: (a) a brief discussion on the Fourth Amendment and *Smith*; (b) a review of Judge Leon's opinion in *Klayman* and an examination on the continuing relevance of *Smith*; and (c) an analysis of the Supreme Court's decision in *Jones*.[212] In turn, each of these issues will be described separately.

a. Judge Collyer's Analysis of the Fourth Amendment and *Smith*

Prior to engaging in her Fourth Amendment analysis, Judge Collyer noted that Judge Leon's reasoning in *Klayman* was "unpersuasive" and "provides no basis for vacating or muddying" the FISC's previously issued production order.[213] Next, Judge Collyer reiterated the Supreme Court's holding in *Smith* that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"[214] and stated that "[o]ther courts have relied on *Smith* in concluding that the Fourth Amendment does not apply to 'trap and trace' devices, which function like pen registers but record the originating numbers of incoming calls, or to information such as the date, time, and duration of calls."[215] Judge Collyer found that the telephone metadata information that petitioner provides the NSA in accordance with the production order is "indistinguishable in nature from the information at issue in *Smith* and its progeny,"[216] and "two judges of this [FISC] . . . and two federal

209. *In re Application*, No. BR 14-01, at *3–6.

210. *Id.* at *2.

211. *Id*. at *9–30.

212. *Id.*

213. *Id.* at *9. For opposing viewpoints discussing Judge Collyer's opinion, *compare* Stewart Baker, *Unpersuasive Judicial Punctuation*, WASH. POST, April 27, 2014, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/04/27/unpersuasive-judicial-punctuation/ *with* Randy Barnett, *Another Secret FISA Opinion Disclosed, and a Question for Stewart Baker*, WASH. POST (April 28, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/04/28/another-secret-fisa-opinion-disclosed-and-a-question-for-stewart-baker/.

214. *In re Application*, No. BR 14-01, at *10. (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

215. *Id.* at *10–11 (citing United States v. Reed, 575 F.3d 900, 914 (9th Cir. 2009); United States Telecom Ass'n v. FCC, 227 F.3d 450, 454, 459 (D.C. Cir. 2000); United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990)).

216. *In re Application*, No. BR 14-01 at *11 (The information being provided to the NSA includes dialed and incoming telephone numbers and other numbers pertaining to the placing or routing of calls, the date, time, and duration of calls; however, it does not include the "contents").

district courts have recently concluded that *Smith* is controlling with respect to the bulk telephony metadata produced to NSA."[217]

b. Judge Collyer's Analysis of *Klayman* and the Relevance of *Smith*

Thereafter, Judge Collyer addressed the following four arguments raised by Judge Leon in *Klayman* wherein he concluded that *Smith* does not provide adequate guidance in determining whether there is a constitutionally protected expectation of privacy in telephone metadata provided to telecommunication entities.[218] First, Judge Leon asserted that the U.S. government's telephone metadata collection activity in *Smith* was limited in duration to approximately two weeks, and the NSA program, in contrast, involves the U.S. government collecting and maintaining five-year's worth of data and it might continue this activity "forever."[219]

Second, Judge Leon argued that, "the relationship between the police and the phone company in *Smith* is *nothing* compared to the relationship that has apparently evolved over the last seven years between the Government and the telecom companies,"[220] and citizens most likely do not expect that telecommunication companies should engage with the NSA in a manner that "is effectively a joint intelligence-gathering operation."[221] Third, Judge Leon argued that technological advancements permit the U.S. government to collect and retain information through means that could not have been "conceived in 1979" and to do so in a manner that evades the "ordinary checks that constrain abusive law enforcement practices."[222] Fourth, Judge Leon found, "most importantly," that "the nature and quantity" of information within telephony metadata "is much greater" today than it was at the time of *Smith*,[223] and

217. *Id.* at *11–12 (citing ACLU v. Clapper, 959 F. Supp. 2d 724, 749–52 (S.D.N.Y. 2013); United States v. Moalin, No. 10cr4246 JM, WL 6079518, at *7–8 (S.D. Cal. Nov. 18, 2013); *In re* Application of the F.B.I., No. BR 13-158 at *5–6.; *In re* Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13–109, 2013 WL 5741573, at *4–5 (FISA Ct. Aug. 29, 2013)). *See also* Press Release, Director of National Intelligence, DOJ and the ODNI Announce the Publication of Additional FISC Filings, Opinions and Orders Regarding Collection Under Section 501 of the FISA (April 25, 2014), http://www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1058-doj-and-the-odni-announce-the-publication-of-additional-fisc-filings,-opinions-and-orders-regarding-collection-under-section-501-of-the-fisa (discussing Judge Collyer's application of Smith in the bulk telephone metadata context) [hereinafter, "Press Release"].

218. *In re* Application of the F.B.I., No. BR 14-01 at *12–14.

219. *Id*. at *12–13 (quoting Klayman v. Obama, 957 F. Supp. 2d 1, 32 (D.D.C. 2013)).

220. *Id.* (quoting *Klayman*, 957 F. Supp. 2d at 32) (emphasis in original).

221. *Id.* at *5 (quoting *Klayman*, 957 F. Supp. 2d at 33).

222. *Id.* at *13–14 (quoting *Klayman*, 957 F. Supp. 2d at 33).

223. *Id.* at *14 (quoting *Klayman*, 957 F. Supp. 2d at 34).

today's metadata can "reveal an entire mosaic-a vibrant and constantly updating picture of the person's life."[224]

After putting forth these arguments, Judge Collyer noted that the FISC "respectfully disagrees with Judge Leon's reasons for deviating from *Smith*."[225] In the words of one commentator, Judge Collyer addressed Judge Leon's decision in *Klayman* and "made short work of it, laying out and rejecting each of Judge Leon's reasons for treating the program as a [F]ourth [A]mendment violation."[226] Specifically, Judge Collyer found that Judge Leon's arguments "focused largely on what happens (and what could happen) to the telephony metadata after it has been acquired by NSA,"[227] and held that this focus is misplaced because the third-party principle makes clear that an individual "has 'no legitimate expectation of privacy in information he voluntarily turns over to third parties' . . . regardless of the disclosing person's assumptions or expectations with respect to what will be done with the information following its disclosure."[228]

The individual disclosing the information "assumes the risk of further disclosure by the third party"[229] and the Court has ruled that it is "unreasonable" for him "to expect his . . . records to remain private."[230] Judge Collyer relied upon this line of reasoning to conclude the following:

> "If a person who voluntarily discloses information can have no reasonable expectation concerning limits on how the recipient will use or handle the information, it necessarily follows that he or she also can harbor no such expectation with respect to how the Government will use or handle the information after it has been divulged by the recipient. *Smith* itself makes clear that once a person has voluntarily conveyed dialing information to the telephone company, he forfeits his right to privacy in the information, regardless of how it might be later used by the recipient or the Government. Accordingly, Judge Leon's concerns regarding NSA's retention and analysis of the call detail records are irrelevant in determining whether a Fourth Amendment search has occurred."[231]

224. *In re Application of the F.B.I.,* No. BR 14-01 at *14 (quoting *Klayman*, 957 F. Supp. 2d at 36).

225. *Id.* at *14.

226. Baker, *supra* note 213.

227. *In re Application* of the F.B.I., No. BR 14-01, at *14.

228. *Id.* at *15 (quoting Smith v. Maryland, 442 U.S. 735, 743–744 (1979)).

229. *Id.* (citing *Smith*, 442 U.S. at 744).

230. *Id.*

231. *Id.* at 17 (internal citations omitted); s*ee generally* Charlie Savage, *Surveillance Court Rules That N.S.A. Can Resume Bulk Data Collection*, N.Y. TIMES, June 30, 2015 (briefly noting that Judge Collyer "rejected Judge Leon's reasoning" in Klayman and "permitted the [telephone metadata collection] program to keep going").

Next, Judge Collyer found that "[f]or the same reason, Judge Leon's assertions regarding citizens' expectations with respect to the 'relationship . . . between the Government and the telecom companies,' also provide no basis for departing from *Smith*."[232] According to Judge Collyer, *Smith* and other judicial precedent on the third party doctrine provides that "any such expectations or assumptions on the part of telephone users who have disclosed their dialing information to the phone company have no bearing on the question whether a search has occurred."[233]

Further, Judge Collyer dismissed Judge Leon's reasoning that the "nature and quantity" of telephone metadata today serves as a basis for deviating from *Smith*.[234] Here, Judge Collyer focused on the incongruity within Judge Leon's argument wherein he asserts that telephone's today, unlike at the time of *Smith*, serve as "'multi-purpose devices' that can be used to access Internet content, and as maps, music players, cameras, text messaging devices,"[235] but simultaneously acknowledges that the type of information acquired by the U.S. government here is limited in scope, such as to the telephone numbers dialed, the length of the call, and the date and time of the call.[236] Therefore, according to Judge Collyer, none of the additional functions equipped on today's phones generate information that the U.S. government is collecting as part of the FISC's production order, and such changes in telephone technology are "irrelevant" to the Fourth Amendment analysis.[237]

Thereafter, Judge Collyer indicated that Judge Leon's "repeated emphasi[s] [on] the total quantity of telephony metadata obtained and retained by NSA" was "misplaced under settled Supreme Court precedent."[238] According to the FISC Judge, given that Fourth Amendment rights are "personal rights" that "may not be vicariously asserted," the "aggregate scope of the collection and the overall size of NSA's database are immaterial in assessing whether any person's reasonable expectation of privacy has been

232. *Id.* (quoting Klayman v. Obama, 957 F. Supp. 2d 1, 32–33 (D.D.C. 2013)).

233. *In re Application of the F.B.I.*, No. BR 14-01, at *18 (citing *Smith*, 442 U.S. at 744); *see* Press Release, *supra* note 217 (noting that Judge Collyer found that Judge Leon's opinion in *Klayman* "was unpersuasive [and] provided no basis for vacating the production order," and "that [*Smith*] is the controlling precedent").

234. *Id.* at *18.

235. *Id.* at *18–19 (quoting *Klayman*, 957 F. Supp. 2d at 34, 36).

236. *Id.* at *18.

237. *Id.* at *19; *see* Kerr, *supra* note 111 (arguing that changes in cell phone technology does not alter the Fourth Amendment analysis in the context described herein because the information the U.S. government collects as part of the telephone metadata program is substantially similar to the types of information collected in *Smith*).

238. *In re Application of F.B.I.*, No. BR 14-01, at *19–20.

violated. . . . ."[239] "The pertinent question," according to Judge Collyer, is "whether a particular user has a reasonable expectation of privacy in the telephony metadata associated with his or her own calls"[240] and in determining whether a search has occurred within the meaning of the Fourth Amendment, "it is irrelevant that other users' information is also being collected and that the aggregate amount acquired is very large."[241]

According to Judge Collyer, "time and technology" have not affected Supreme Court precedent, and the government's collection program under review is less intrusive then the one the government reviewed in *Miller*, which was the principal case relied upon in *Smith*.[242] In *Miller*, the Supreme Court held that a bank customer did not have a legitimate expectation of privacy in bank records that provided to police investigators pursuant to a subpoena and included checks, deposit slips, monthly statements and financial statements for a span of over three months.[243] The Court found that the bank records "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business"[244] and that "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[245] According to Judge Collyer, "[i]t is far from clear to this Court that even years' worth of non-content call detail records would reveal more of the details about a telephone user's personal life than several months' worth of the same person's bank records."[246]

"[B]ank records," according to the Judge, "are likely to provide the Government *directly* with detailed information about a customer's personal life,"[247] such as the identities of the individuals with whom the customer has had financial relationships, the sources of his personal income, the amounts and detailed types of his personal expenses, the charities and political organizations he supports through financial donations – all of which is

239. *Id.* at *20 (citing Rakas v. Illinois*,* 439 U.S. 128, 133–34 (1978); Minnesota v. Carter, 525 U.S. 83, 88 (1998)); *see also* White Paper, *supra* note 23, at 20 (noting that the volume of records collected by the U.S. government does not alter its Fourth Amendment analysis).

240. *In re Application of the F.B.I*, No. BR 14-01, at *20.

241. *Id. See* Charlie Savage, *Phone Company Bid to Keep Data From N.S.A. Is Rejected*, N.Y. TIMES (April 25, 2014) ("Judge Collyer said the Supreme Court precedent was still valid and that the bulk nature of the collection was irrelevant because what mattered was each individual caller's expectation of privacy.").

242. *In re Application of the F.B.I*, No. BR 14-01, at *21, 23.

243. *Id.* at *21 (citing United States v. Miller, 425 U.S. 435, 443, 448 (1976)); *see generally* Kerr, *supra* note 52, at 578–79 (discussing *Miller* and the third party doctrine).

244. *In re Application of F.B.I.*, No. BR 14-01 at *21 (quoting *Miller,* 425 U.S. at 442).

245. *Id.* at *21 (quoting *Miller*, 425 U.S. at 433).

246. *Id.*

247. *Id.* (emphasis in original).

information "that call detail records simply do not, by themselves, provide."[248] Separately, Judge Collyer reasoned that the *Miller* decision, which was published in 1976, "substantially undermines Judge Leon's conclusion that *Smith* does not apply to the NSA telephony metadata program because the metadata from each person's phone reveals so much about a person 'that could not have been gleaned from a data collection in 1979,' when *Smith* was decided."[249] The Judge found that "[m]any more personal details" could be uncovered from bank records such as the ones approved by the *Miller* Court without raising expectation of privacy concerns.[250]

c. Judge Collyer's Analysis of *Jones*

After addressing the aforementioned arguments raised by Judge Leon in *Klayman*, Judge Collyer turned to the issue of whether the Supreme Court's decision in *Jones* altered whether there is a constitutionally protected expectation of privacy in telephone metadata.[251] She noted that the Supreme Court's holding therein rested on the fact that the U.S. government obtained the information in question through a physical intrusion on the defendant's vehicle, which the Court viewed as a constitutionally-protected area.[252] Judge Collyer emphasized that the Supreme Court cited *Smith* "only in passing" in the *Jones* case.[253]

She also noted that although there are two concurring opinions in *Jones* that address privacy issues, "they suggest distinct analytical approaches and thus can hardly be read as having adopted a single, coherent principle or methodology for lower courts to apply."[254] First, with regard to Justice Sotomayor's concurrence in *Jones*, the Associate Justice's opinion focused on whether police conduct collected so much personal information on an individual that it enabled law enforcement to learn about a person's private affairs at any given time.[255] Second, Justice Alito's opinion framed the issue as whether the police investigation at issue exceeded society's expectations for how law enforcement personnel would in fact investigate a particular crime.[256] Judge Collyer emphasized that Justice Alito's concurrence, to which three

248. *Id.* at *21–22.

249. *Id.*

250. *Id.* at *22; *but see* Barnett, *supra* note 213 (criticizing the analogy to bank records, as described in *Miller*, in the telephone metadata context).

251. *In re Application of F.B.I.*, No. BR 14-01 at *24.

252. *Id*. at *25 (citing United States v. Jones, 132 S. Ct. 945, 949, 953 (2012)).

253. *Id.* at. *26 (citing *Jones,* 132 S. Ct. at 950).

254. *Id.* at *26–27.

255. *Id.* at *27 (citing Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 328 (Dec. 2012)).

256. *Id.* (citing Kerr, *supra* note 255, at 328).

other Justices joined, does not even mention *Smith*.[257] Also, she stated the distinct approaches taken in the concurring opinions "undercut Judge Leon's suggestion that the five concurring Justices in *Jones* can be viewed as a *de facto* majority on the issue."[258]

Judge Collyer reiterated that although Justice Sotomayor stated in her concurrence "that 'it may be necessary to reconsider" the third-party disclosure principle applied in *Smith* and *Miller,* which she described as 'ill suited to the digital age,' she expressly stated that it was unnecessary for the Court to undertake such a reexamination in *Jones*."[259] Thus, "[w]hile the concurring opinions in *Jones* may signal that some or even most of the Justices are ready to revisit certain settled Fourth Amendment principles, the decision in *Jones* itself breaks no new ground concerning the third-party disclosure doctrine generally or *Smith* specifically."[260]

4. *In re Application* (June 2015 Opinion)

In June of 2015, Judge Mosman, writing on behalf of the FISC, addressed whether to approve an application by the FBI requiring the production of certain telephone metadata in light of the recently-enacted USA FREEDOM Act.[261] Judge Mosman found that the FISC was authorized to approve such requests, at least for an interim period of 180-days until certain provisions within the USA FREEDOM Act that ended the government's bulk collection of telephone metadata went into effect.[262] According to one commentator, the 180-day transition period was "baked into" the law "to allow the NSA time to switch over to a more limited and targeted surveillance regime."[263]

Prior to reviewing whether the bulk telephone metadata collection program was consistent with the Fourth Amendment, Judge Mosman analyzed the underlying statutory authority for the U.S. government to request and collect

257. *In re Application of F.B.I.*, No. BR 14-01 at *27–28.

258. *Id.* at *27 (citing Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013)); United States v. Jones, 132 S. Ct. 945, 957 (2012) (Alito, J., concurring).

259. *In re Application of F.B.I.*, No. BR 14-01 at *28 (quoting United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring)).

260. *Id.* at *30. Judge Collyer also stated, "[t]he concurring opinions notwithstanding, *Jones* simply cannot be read as inviting the lower courts to rewrite Fourth Amendment law in this area." *Id.*

261. In re Application of the F.B.I. for an Order Requiring the Production of Tangible Things, No. BR 15-75, at *1 (FISC Ct. June 29, 2015) (internal citations omitted).

262. *Id.*

263. Dustin Volz, *Court Revives Defunct NSA Mass Surveillance Program*, Nat'l J. (June 30, 2015), http://www.nationaljournal.com/s/24869/court-revives-defunct-nsa-mass-surveillance-program; *see also Statement by the ODNI on Retention of Data Collected Under Section 215 of the USA PATRIOT Act*, IC on the Rec. (July 27, 2015) (discussing how the U.S. government will retain and access telephone metadata previously collected in accordance with Section 215), http://icontherecord.tumblr.com/post/125179645313/statement-by-the-odni-on-retention-of-data.

the bulk telephone metadata in question.[264] Specifically Judge Mosman addressed the conclusion reached by the Second Circuit Court of Appeals in *Clapper* that section 215 of the USA PATRIOT ACT does not permit the FISC to approve applications permitting the U.S. government to collect vast amounts of telephone data.[265] Specifically, Judge Mosman found that "Second Circuit rulings are not binding on the FISC,"[266] the FISC "disagrees with the [Second Circuit's] analysis,"[267] and "[t]o a considerable extent, the Second Circuit's analysis rests on mischaracterizations of how [the telephone metadata collection] program works. . . "[268] The Judge's opinion led one commentator to claim that there was a "cat fight between the FISA court and the 2nd Circuit Court of Appeals."[269]

In turning to his Fourth Amendment analysis, Judge Mosman noted that "the FISC has repeatedly concluded on numerous occasions that NSA's acquisition of call detail records under the terms set forth in the government's application . . . comports with the Fourth Amendment to the Constitution."[270] He then addressed the argument raised by amici that the "differences between the present circumstances and *Smith* in nature and scope are so stark as to make *Smith* inapposite,"[271] and responded by holding that the nature of the information government receives pursuant to the FISC's order, which does not include any communications content, is "indistinguishable from the information at issue in *Smith* and its progeny."[272] Judge Mosman found, "[a]s in *Smith*, this information is voluntarily conveyed to a telecommunications provider when a person places a call, and the provider stores and uses the information for billing and other purposes."[273]

The FISC Judge addressed that fact that, unlike in *Smith*, the government was using the FISC's order to collect "trunk identifiers," "International Mobile Subscriber Identity" numbers, "International Mobile station Equipment Identity" numbers and telephone calling card numbers, and ruled that such information is still the same type of dialing, signaling, and routing information that that does not include communications contents and that telephone users provide to telecommunication entities in order to complete routine calls and

264. *In re Application of F.B.I.*, No. BR 15-75, at *8–18.

265. *Id.* at *11

266. *Id.* at *14–15.

267. *Id.* at *15.

268. *Id.* at *16.

269. Benjamin Wittes, *Rational Security, the "War on the War on Terror" Edition*, LAWFARE (July 2, 2015, 10:03 AM), https://www.lawfareblog.com/rational-security-war-war-terror-edition.

270. *In re Application of F.B.I.*, No. BR 15-75, at *12.

271. *Id.* at *18.

272. *Id.*

273. *Id.* at *20.

which is retained for business purposes.[274] Judge Mosman found that users of such telecommunications services simply have no reasonable expectation of privacy in this information.[275]

Without going into more detail, Judge Mosman dismissed other arguments raised by the Movants related to the "nature of the produced call detail records" on the grounds that Judge Collyer "previously considered and rejected" these arguments.[276] Judge Mosman also cited Judge Collyer's opinion as he rejected the attempt "to distinguish this case [from *Smith*] based on the government's storage and use of the data post-acquisition" because the "third-party disclosure principle applies regardless of the disclosing person's assumptions or expectations with respect to what will be done with the information following its disclosure."[277] Next, Judge Mosman again relied on Judge Collyer's previous opinion to summarily reject (without more explanation) the Movants' arguments that the FISC should find a reasonable expectation of privacy in the metadata provided to telecommunications entities because of "expectations based on their contractual relationships with telecommunications providers, the fact that there are more providers to choose from than there were in 1979, and . . . that the relationship between the government and the providers is different."[278]

Thereafter, Judge Mosman stated that the argument that "the scope of the collection justifies departing from *Smith*" was "equally unavailing."[279] Specifically, Judge Mosman cited the principle that "Fourth Amendment rights 'are personal in nature'"[280] to reason that the government's acquisition of "data about many people is immaterial in assessing whether any particular person's reasonable expectation of privacy has been violated such that a search under the Fourth Amendment has occurred.[281] "To the extent the quantity of metadata is relevant at all, it can only be the quantity of metadata that pertains to a particular person," according to the Judge.[282]

274. *Id.*

275. *Id. See generally* Lauren Walker, *NSA to Keep Collecting Your Telephone Metadata for 6 More Months, Court Rules,* NEWSWEEK (June 30, 2015, 3:20 PM), http://www.newsweek.com/nsa-keep-collecting-your-telephone-metadata-6-more-months-court-rules-348847.

276. *In re Application of F.B.I.*, No. BR 15-75, at *20.

277. *Id.* at *20–21.

278. *Id.* at *21 (citing *In re Application of the F.B.I.*, No. 14-01, at *16, *17–18); *see generally* Savage, *supra* note 195.

279. *In re Application of F.B.I.*, No. BR 15-75, at *22.

280. *Id.*

281. *Id.* (citing *In re Application of the F.B.I.*, No. BR 14-01 at *20).

282. *Id.* at *22 (citing *In re Application of the F.B.I.*, No. BR 14-01 at *20–21); *see also* White Paper, *supra* note 23, at 20 (noting that the volume of records collected by the U.S. government does not alter its Fourth Amendment analysis).

In a separate portion of his analysis, Judge Mosman reiterated the Movants' argument "that a series of statutes enacted after *Smith* respecting the disclosure by telephone companies of information about their customers' calls supports the conclusion that Movants have a reasonable expectation of privacy in the metadata in question" and found that this argument "lacks merit."[283] According to the FISC Judge, Congress may provide safeguards to personal information and regulate how law enforcement personnel access and retain such data.[284] However, according to the Judge, this type of legal framework is statutory (and not constitutional) in nature, and thus does not impact the Fourth Amendment's search and seizure framework.[285] The Judge also noted that the actual statutes cited by movants "fail" to even support their Fourth Amendment argument.[286]

Next, Judge Mosman rejected the Movants' argument that the FISC should interpret certain case law to find the third-party disclosure inapplicable to the current case, and ruled that "these cases do not reduce the binding authority of *Smith*"[287] and that the FISC previously addressed and distinguished several of the cases raised by the Movants.[288] Next, and just as hastily, the Judge rejected the movants argument related to the U.S government's collection of cell-site and GPS location information on the ground that "no such information is involved in this case."[289]

Last, Judge Mosman concluded his Fourth Amendment legal analysis by addressing the Movant's argument that the FISC "should find that they have a reasonable expectation of privacy in call detail records based on the concurring opinions in [*Jones*]."[290] The Judge noted that two FISC judges – Judge Collyer and Judge McLaughlin – previously heard similar arguments and rejected them for lack of merit, respectively, and he "agrees with their analysis."[291] Specifically, Judge Mosman quoted Judge Collyer's opinion in support of the following proposition: "[w]hile the concurring opinions in *Jones* may signal that some or even most of the Justices are ready to revisit certain settled Fourth

283. *In re Application of F.B.I.*, No. BR 15-75, at *22–23.

284. *Id.* at *23.

285. *Id. See* United States v. Kington, 801 F.2d 733,737 (5th Cir. 1986) (rejecting claim that enhanced protections for bank records in Right to Financial Privacy Act impact expectations of privacy within the context of the Fourth Amendment).

286. *In re Application of F.B.I.*, No. BR 15-75, at *23.

287. *Id.*

288. *Id*. (citing *In re Application of the F.B.I.*, No. BR 14-01, at *16, *18).

289. *Id.* at *24. Smith v. Obama*,* 24 F.Supp. 3d 1005, 1008–09 (D. Idaho 2014) (noting that the "subject lurking in the shadows" was the "possibility that the NSA is tracking the location of calls"). However, the Chief Judge concluded that "[w]hile there is speculation that the NSA is tracking location, there is no evidence of that, and the agency denies it" and "the Court will not assume that the NSA's privacy intrusions include location tracking." *Id.* at 1009.

290. *In re Application of F.B.I.*, No. BR 15-75, at *24.

291. *Id.*

Amendment principles, the decision in *Jones* itself breaks no new ground concerning the third-party disclosure doctrine generally or *Smith* specifically . . . "[292] Thus, Judge Mosman found that because *Smith* was controlling and the U.S. government's collection of telephone metadata in accordance with Section 215 did not implicate the Fourth Amendment.[293]

V. CONCLUSION

The aforementioned cases represent the most recent legal opinions discussing whether the Fourth Amendment impacts the U.S. government's ability to collect and retain telephone metadata in bulk. Given the recent statutory amendments enumerated in the USA FREEDOM ACT[294] and the probability that without additional congressional action the U.S. government may no longer use Section 215 of the USA PATRIOT ACT[295] to collect telephone metadata in bulk, the cases discussed herein may become moot and dismissed in the near future. Thus, this case law may provide the most relevant precedent for years to come on the issue of whether individuals have a constitutionality protected reasonable expectation of privacy in telephone metadata.

In discussing this issue, the cases described in Part IV of this article primarily focus on whether *Smith's* holding that a telephone user does not have an expectation of privacy in a limited amount of telephone metadata provided to a telephone company is applicable to an exponentially greater volume of the same information. As noted above, Judge Leon would seem to answer that question in the negative[296], as would Supreme Court Justice Sotomayor.[297] According to their opinions described *supra*, such voluminous amounts of telephone metadata reveals deeply personal information and, through the last several years, society has come to expect that such private and personal information would not be readily available to the U.S. government in a manner outside the scope and restrictions enumerated in the Fourth Amendment.[298]

However, these arguments have been thoroughly rejected by the FISC and have not fared too well in other Article III courts. For example, courts have rejected these arguments for the following reasons: an individual should not

292. *Id.* at *24–25 (quoting *In re Application of the F.B.I.*, No. 14-01, at *30).

293. *Id.* at *25.

294. Pub. L. No. 114–23, 129 Stat. 268 (2015).

295. *See* United States v. Moalin, No. 10cr4246 JM, slip op., 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013); Klayman v. Obama, 957 F. Supp. 2d 1, 11–14 (D.D.C. 2013); ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); Smith v. Obama, 24 F.Supp. 3d 1005 (D. Idaho 2014); In re Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13–109, 2013 WL 5741573 (FISA Ct. Aug. 29, 2013).

296. *See Klayman*, 957 F. Supp. 2d at 33.

297. *See* Part IV, *infra*.

298. *Id*.; Klayman v. Obama, 957 F. Supp. 2d 1.

reasonably expect that information he provides a third party will remain private or in confidence of the recipient; the type of information that the U.S. government collected pursuant to Section 215, non-content-based information, is substantially similar to the information at issue in *Smith*, which therefore should remain controlling; information not protected by the Fourth Amendment, such as non-content based telephone metadata, does not gain such protection simply because one aggregates that information large amounts; and the Constitution does not protect other types of information beyond telephone metadata that reveals deeply personal information, such as bank records, and thus it would not be appropriate to extend the Fourth Amendment to telephone metadata provided to third parties.[299]

As is clear from the case summary provided herein, the judges addressing this very difficult constitutional issue put forth valid and respectable arguments in which one can reasonable and ethically agree or disagree. However, as noted, this issue may not be resolved by the Supreme Court in the near term, and it will be lawyers and practitioners that will need to rely on this case law in developing their own arguments regarding the applicability of the Fourth Amendment as similar national security programs that are developed in the future.

299. *See* United States v. Moalin, No. 10cr4246 JM, slip op., 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013); Klayman, 957 F. Supp. at 21; ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); Smith v. Obama, 24 F.Supp. 3d 1005 (D. Idaho 2014); In re Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13–109, 2013 WL 5741573 (FISA Ct. Aug. 29, 2013).